

Unambiguous State Discrimination of two density matrices in Quantum Information Theory

Den Naturwissenschaftlichen Fakultäten
der Friedrich-Alexander-Universität Erlangen-Nürnberg
zur
Erlangung des Doktorgrades

vorgelegt von
Philippe Raynal
aus Lyon, Frankreich

Quantum Information Theory Group
Theoretische Physik I

Lehrstuhl für Optik
Institut für Optik, Information und Photonik
Max Planck Forschungsgruppe

Erlangen 2006

Als Dissertation genehmigt von den naturwissenschaftlichen Fakultäten der Universität
Erlangen-Nürnberg

Tag der mündlichen Prüfung:

16.08.2006

Vorsitzender der Promotionskommission:

Prof. Dr. D. P. Häder

Erstberichterstatte:

Prof. Dr. N. Lütkenhaus

Zweitberichterstatte:

Prof. Dr. D. Bruß

Abstract

Quantum state discrimination is a fundamental task in quantum information theory. The signals are usually nonorthogonal quantum states, which implies that they can not be perfectly distinguished. One possible discrimination strategy is the so-called Unambiguous State Discrimination (USD) where the states are successfully identified with non-unit probability, but without error. The optimal USD measurement has been extensively studied in the case of pure states, especially for any pair of pure states. Recently, the problem of unambiguously discriminating mixed quantum states has attracted much attention. In the case of a pair of generic mixed states, no complete solution is known. In this thesis, we first present reduction theorems for optimal unambiguous discrimination of two generic density matrices. We show that this problem can be reduced to that of two density matrices that have the same rank r in a $2r$ -dimensional Hilbert space. These reduction theorems also allow us to reduce USD problems to simpler ones for which the solution might be known. As an application, we consider the unambiguous comparison of n linearly independent pure states with a simple symmetry. Moreover, lower bounds on the optimal failure probability have been derived. For two mixed states they are given in terms of the fidelity. Here we give tighter bounds as well as necessary and sufficient conditions for two mixed states to reach these bounds. We also construct the corresponding optimal measurement. With this result, we provide analytical solutions for unambiguously discriminating a class of generic mixed states. This goes beyond known results which are all reducible to some pure state case. We however show that examples exist where the bounds cannot be reached. Next, we derive properties on the rank and the spectrum of an optimal USD measurement. This finally leads to a second class of exact solutions. Indeed we present the optimal failure probability as well as the optimal measurement for unambiguously discriminating any pair of geometrically uniform mixed states in four dimensions. This class of problems includes for example the discrimination of both the basis and the bit value mixed states in the BB84 QKD protocol with coherent states.

Zusammenfassung

Quantenzustandsunterscheidung ist eine fundamentale Aufgabe der Quanteninformationstheorie. Die Signale sind normalerweise nicht-orthogonale Quantenzustände, d.h. sie können nicht perfekt unterschieden werden. Eine der möglichen Unterscheidungsstrategien ist die so genannte Eindeutige Zustandsunterscheidung (Unambiguous State Discrimination - USD), bei der die Zustände mit einer Wahrscheinlichkeit kleiner als eins erfolgreich erkannt werden, allerdings fehlerfrei. Optimale USD-Messungen für reine Zustände sind ausführlich untersucht worden, insbesondere für jedes Paar von reinen Zuständen. Vor kurzem hat die Aufgabenstellung der eindeutigen Zustandsunterscheidung gemischter Zustände viel Aufmerksamkeit auf sich gezogen. Im Falle eines Paares von allgemeinen gemischten Zuständen ist keine vollständige Lösung bekannt. In dieser Doktorarbeit legen wir zuerst Reduktionstheoreme für optimale eindeutige Unterscheidung von zwei allgemeinen Dichtematrizen vor. Wir zeigen, dass diese Aufgabenstellung reduziert werden kann auf diejenige von zwei Matrizen, die denselben Rang r in einem $2r$ -dimensionalen Hilbert-Raum haben. Diese Reduktionstheoreme ermöglichen uns ebenfalls, USD-Aufgaben auf einfachere zurückzuführen, für die die Lösung möglicherweise bekannt ist. Der eindeutige Vergleich von n linear abhängigen reinen Zuständen mit einfacher Symmetrie wird als Anwendung behandelt. Darüber hinaus wurden untere Grenzen für die optimale Fehlerwahrscheinlichkeit entwickelt. Für zwei gemischte Zustände werden diese in Form der Fidelity angegeben. Hier geben wir engere Grenzen an, ebenso wie notwendige und ausreichende Bedingungen für zwei gemischte Zustände, diese Grenzen zu erreichen. Wir konstruieren ebenfalls die entsprechende optimale Messung. Zusammen mit diesem Ergebnis präsentieren wir analytische Lösungen für die eindeutige Unterscheidung einer Kategorie allgemeiner gemischter Zustände. Dies geht über bekannte Ergebnisse hinaus, die alle auf reine Zustände zurückführbar sind. Wir zeigen allerdings, dass es Beispiele gibt, bei denen die Grenzen nicht erreicht werden können. Als nächstes leiten wir Eigenschaften des Rangs und des Spektrums einer optimalen USD-Messung her. Dies führt schließlich zu einer zweiten Kategorie exakter Lösungen. Wir zeigen die optimale Fehlerwahrscheinlichkeit auf, ebenso wie die optimale Messung, um jedes Paar geometrisch gleichförmiger gemischter Zustände in vier Dimensionen zu unterscheiden. Diese Kategorie von Aufgabenstellungen schließt zum Beispiel die Unterscheidung von sowohl der basis- als auch der bit value-gemischten Zustände des BB84-QKD-Protokolls mit kohärenten Zuständen ein.

Contents

Abstract	v
Zusammenfassung	vii
1 Prologue	1
1.1 Quantum Information Theory	1
1.1.1 Ensemble of quantum states and density matrix	2
1.1.2 Generalized measurements - POVM	3
1.1.3 Definitions and notations	4
1.2 Unambiguous Quantum State Discrimination	5
1.3 Results	9
2 Optimal Unambiguous State Discrimination	15
2.1 The USD measurement	15
2.2 Solution for two pure states	17
2.3 Solution for n symmetric pure states	19
2.4 Necessary and sufficient conditions for the optimality of a USD measurement	19
2.5 Bounds on the failure probability	20
2.5.1 Fidelity	20
2.5.2 Lower bound for the unambiguous discrimination of n mixed states	21
2.5.3 Lower and upper bounds on the failure probability for the unambiguous discrimination of two mixed states	22
3 A standard form	25
3.1 Overlapping supports	26
3.2 Trivial orthogonal subspaces of the supports	29
3.3 Block diagonal structure	34
3.4 A standard form of USD problem	37
3.5 Applications of the reduction theorems	39
3.5.1 State Filtering	39

3.5.2	Unambiguous Subspace Discrimination	41
3.5.3	Unambiguous State Comparison	44
4	First class of exact solutions	57
4.1	Lower bounds on the failure probability	57
4.2	Parallel addition $\rho_0 \Sigma^{-1} \rho_1$	63
4.3	Necessary and sufficient conditions - first class of exact solutions	64
4.4	The two pure states case revisited	67
5	Second class of exact solutions	73
5.1	Overall lower bound and rank of the POVM elements	73
5.2	Maximum rank and <i>a priori</i> probabilities	77
5.3	A fourth, incomplete, reduction theorem	79
5.4	Second class of exact solutions	83
5.4.1	Geometrically uniform states	83
5.4.2	Optimal unambiguous discrimination of two geometrically uniform states in four dimensions	84
6	Application of the second class of exact solutions to the BB84 protocol	89
6.1	Two geometrically uniform states in a four-dimensional Hilbert space	91
6.2	USD of the <i>basis</i> mixed states	97
6.3	USD of the <i>bit value</i> mixed states	102
7	Epilogue	111
8	Appendix	115
8.1	Appendix A	115
8.2	Appendix B	115
8.3	Appendix C	116
	Bibliography	119
	Curriculum Vitae	123

List of Figures

1.1	Two parties Alice and Bob want to communicate	6
1.2	Two possible outcomes in the scenario of Minimum Error Discrimination	7
1.3	Three possible outcomes in the scenario of Unambiguous State Discrimination .	8
2.1	Optimal failure probability for USD of two pure states	18
2.2	Basis vectors $ \Psi_1^\perp\rangle$, $ \Psi_0^\perp\rangle$ and $?\rangle$ of the three POVM elements E_0 , E_1 and $E_?$ for the optimal USD measurement of two pure states when $\langle\Psi_0 \Psi_1\rangle \geq 0$ and $ \langle\Psi_0 \Psi_1\rangle \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{ \langle\Psi_0 \Psi_1\rangle }$	18
2.3	Lower bounds on the optimal failure probability for USD of two density matrices	23
3.1	Illustration of a common subspace between ρ_0 and ρ_1	27
3.2	Illustration of the subspace $\mathcal{H}_{\rho_0} \cap \mathcal{S}_{\rho_1}$	31
5.1	A constructive way to solve any USD problem (the exponent (r) denotes the rank of the density matrices after reduction)	81
6.1	Schematic view of the four symmetric states in the phase space	93
6.2	Pairing of the four symmetric states for the <i>basis</i> mixed states	94
6.3	Pairing of the four symmetric states for the <i>bit value</i> mixed states	95
6.4	Third possible pairing of the four symmetric states	97
6.5	Optimal failure probability for USD of the <i>basis</i> mixed states	101
6.6	Spectrum of the operator $\rho_0 - F_0$ for USD of the <i>bit value</i> mixed states	107
6.7	Optimal failure probability for USD of the <i>bit value</i> mixed states for $\mu \geq \mu_0$. . .	107
6.8	Optimal failure probability for USD of the <i>bit value</i> mixed states	108
6.9	Comparison between the optimal failure probabilities for USD of the <i>basis</i> and the <i>bit value</i> mixed states	109

Chapter 1

Prologue

Physics attempts to describe the world with the language of mathematics. Given a system an observer summarizes his knowledge in an abstract mathematical object, the so-called 'state'. At a given point in time this observer may decide to acquire information about the system. Such an acquisition of information is called a measurement. In that sense, Quantum Mechanics is concerned with knowledge, and the two pillars of Quantum Mechanics are *states* and *measurements*.

Information Theory started in the late 1940's boosted by the second world war and its needs for communication and computational power. Information Theory addresses the fundamental questions of the transmission, processing and coding of information.

It is therefore quite natural that Quantum Mechanics and Information Theory finally merge to describe the production, the transmission and the detection of information as well as its processing and coding. Quantum Information Theory was born.

1.1 Quantum Information Theory

Since no information-theoretic formulation¹ is yet available, Quantum Information Theory (QIT) is formulated on the basis of four postulates that mathematically describe a physical system, its evolution and measurements that can be performed on it. Let us now review these four postulates [1].

Postulate 1 *Hilbert space*

Associated to any isolated quantum system is a Hilbert space known as the state space of the system. The system is completely described by a unit vector $|\Psi\rangle$ called the state vector in the state space.

¹See the work of R. Clifton, J. Bub and H. Halvorson or the work of A. Grinbaum for two appealing attempts.

Postulate 2 *Unitary evolution*

The evolution of a closed (i.e. an isolated system having no interaction with the environment) quantum system is described by a unitary transformation. That is, if $|\Psi\rangle$ is the state at time t , and $|\Psi'\rangle$ is the state at time t' , then $|\Psi'\rangle = U|\Psi\rangle$ for some unitary operator U which depends only on t and t' .

Postulate 3 *Measurement*

A measurement is described by a collection $\{M_m\}$ of measurement operators. These operators are acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\Psi\rangle$ immediately before the measurement then the probability that result m occurs is given by $p(m) = \langle\Psi|M_m^\dagger M_m|\Psi\rangle$, and the state of the system after the measurement is $\frac{M_m|\Psi\rangle}{\sqrt{\langle\Psi|M_m^\dagger M_m|\Psi\rangle}}$. Moreover the measurement operators satisfy the completeness equation, $\sum_m M_m^\dagger M_m = \mathbb{1}$.

Note that in Quantum Information Theory the measurement operators $\{M_m\}$ are often called Kraus operators [2].

Postulate 4 *Composite system*

The state space of a composite quantum system is the tensor product of the state spaces of the component quantum systems. That is, if we have systems numbered 1 through n , and system number i is prepared in the state $|\Psi_i\rangle$, then the joint state of the total system is $|\Psi_1\rangle \otimes |\Psi_2\rangle \otimes \cdots \otimes |\Psi_n\rangle$.

Note that, unlike in Quantum Mechanics, observables do not have a crucial role in Quantum Information Theory. Moreover, in general, we can consider the state of a system to be not only a vector state but a classical mixture of vector states. The notion of density matrices then is useful as we will see in the next subsection. Measurements are the core of Quantum Information theory because it is through a measurement that we learn information about a system. Therefore, we also introduce the mathematical language used to describe a measurement.

1.1.1 Ensemble of quantum states and density matrix

Let us suppose a quantum system is in the state $|\Psi_i\rangle$ chosen in a set of states $\{|\Psi_i\rangle\}$. We can imagine that the appearance probabilities η_i of each state of the set are in general different. We then summarize our knowledge on the system with the ensemble $\{|\Psi_i\rangle, \eta_i\}$. It is called an *ensemble of the system*. If the ensemble is composed of only one state (and of course its *a priori* probability equals 1), the state is called *pure*. If not, one speaks of *mixed* states that is to say a classical mixture of pure states. To efficiently describe a *mixed* state, we use an operator instead of a vector state, the so-called density matrix.

Definition 1 *Density matrix*

Let us consider a system with ensemble $\{|\Psi_i\rangle, \eta_i\}$. The state of the system can then be described in a compact form by the density matrix

$$\rho = \sum_i \eta_i |\Psi_i\rangle \langle \Psi_i|. \quad (1.1)$$

Such a density matrix possesses the three important properties

$$\text{Tr}(\rho) = 1 \quad (\text{Normalization}), \quad (1.2)$$

$$\rho \geq 0 \quad (\text{Positivity}), \quad (1.3)$$

$$\text{Tr}(\rho^2) = 1 \quad : \quad \rho = |\Psi\rangle \langle \Psi| \quad (\text{Purity}), \quad (1.4)$$

where ≥ 0 means positive semi-definite. Actually, the state ensemble of a system is not unique.

Theorem 1 *Unitary freedom in the state ensemble*

The sets $\{|\Psi_i\rangle, \eta_i\}$ and $\{|\Phi_i\rangle, \nu_i\}$ generate the same density matrix if and only if there exists a unitary transformation U such that

$$\sqrt{\nu_i} |\Phi_i\rangle = \sum_j U_{ij} \sqrt{\eta_j} |\Psi_j\rangle. \quad (1.5)$$

Equivalently,

Corollary 1 *Unitary freedom in the state ensemble of a density matrix*

The two density matrices $\sum_i \eta_i |\Psi_i\rangle \langle \Psi_i|$ and $\sum_i \nu_i |\Phi_i\rangle \langle \Phi_i|$ describe the same state if and only if there exists a unitary transformation U such that

$$\sqrt{\nu_i} |\Phi_i\rangle = \sum_j U_{ij} \sqrt{\eta_j} |\Psi_j\rangle. \quad (1.6)$$

1.1.2 Generalized measurements - POVM

The third postulate of QIT, and its measurement operators E_m , can be used to define the positive semi-definite operators $E_m = M_m^\dagger M_m$. The set $\{E_m\}_m$ is called a Positive Operator-Valued Measure (POVM) [3, 2, 4] and each operator E_m , a POVM element. On one hand, the fact that the probabilities $p(m) = \langle \Psi | E_m | \Psi \rangle$ are real and positive is expressed by the positivity of the POVM elements $\{E_m\}_m$. On the other hand, the fact that probabilities add up to one is expressed by the completeness relation $\sum_m E_m = \mathbb{1}$. Indeed, the sum of the probability $p(m)$ is $\sum_m p(m) = \sum_m \langle \Psi | E_m | \Psi \rangle = \langle \Psi | \sum_m E_m | \Psi \rangle = \langle \Psi | \Psi \rangle = 1$. An important property of a POVM element is that its spectrum is upper bounded by 1. Otherwise, it is clear that the expectation value $\langle \Psi | E_m | \Psi \rangle$ would exceed unity which contradicts the requirement that a probability is less than 1. We finally give a general definition of a POVM.

Definition 2 *POVM*

A *Positive Operator-Valued Measurement (POVM)* is a set of positive semi-definite operators $\{E_m\}_m$ such that

$$E_k \geq 0 \text{ (Positivity)} \quad (1.7)$$

$$\sum_k E_k = \mathbb{1} \text{ (Completeness relation)} \quad (1.8)$$

The probability to obtain the outcome k for a given state ρ_i is then given by

$$p(k|i) = \text{Tr}(E_k \rho_i). \quad (1.9)$$

In the previous formula, $\text{Tr}(\cdot)$ stands for the trace. A POVM is also called a generalized measurement since it is the most general description of a measurement. Indeed, projective measurements, usually encountered in Quantum Mechanics are, in the above formalism, merely a special case where $E_m E_n = \delta_{mn} E_m$, $E_m^2 = E_m$. Such a projective measurement is called a Projection Valued Measure (PVM). Nevertheless, a generalized measurement can also be described by a projective measurement on an *enlarged* Hilbert space. A generalized measurement is then seen as a special case of projective measurements. The two pictures finally are equivalent as long as the Hilbert space is not fixed. This is made precise in the following theorem due to Naimark [5, 6].

Theorem 2 *Naimark's extension*

Given $\{E_k\}$ a POVM on a Hilbert space \mathcal{H} , it exists an embedding of \mathcal{H} into a larger Hilbert space \mathcal{K} such that the measure can be described by projections onto orthogonal subspaces in \mathcal{K} . That is, there exist a Hilbert space \mathcal{K} , an embedding \mathcal{E} such that $\mathcal{E}\mathcal{H} = \mathcal{K}$ and a PVM $\{R_k\}$ in \mathcal{K} , such that with P , the projection defined by $P\mathcal{K} = \mathcal{H}$, $E_k = PR_kP$, $\forall k$.

1.1.3 Definitions and notations

Here we briefly fix some notations. Throughout this thesis, we will make an extensive use of the support $\mathcal{S}_P := \text{support}(P)$ of a Hermitian operator P . The support of a Hermitian operator is defined as the subspace spanned by its eigenvectors. We can moreover define the kernel $\mathcal{K}_P := \text{kernel}(P)$ of a Hermitian operator P as the subspace orthogonal to its support. We also denote $r_P := \text{rank}(P) = \dim(\mathcal{S}_P)$, the rank of P .

Next we define in a Hilbert space \mathcal{H} the sum and the intersection of two Hilbert subspaces \mathcal{H}_1 and \mathcal{H}_2 . The sum $\mathcal{H}_1 + \mathcal{H}_2$ of the subspaces \mathcal{H}_1 and \mathcal{H}_2 is defined to be the set consisting of all sums of the form $a_1 + a_2$, where $a_1 \in \mathcal{H}_1$ and $a_2 \in \mathcal{H}_2$. $\mathcal{H}_1 + \mathcal{H}_2$ is a Hilbert subspace of \mathcal{H} . The intersection $\mathcal{H}_1 \cap \mathcal{H}_2$ is defined to be the set consisting of all the elements a , where $a \in \mathcal{H}_1$ and $a \in \mathcal{H}_2$. $\mathcal{H}_1 \cap \mathcal{H}_2$ is a Hilbert subspace of \mathcal{H} . The complementary orthogonal subspace (or orthogonal complement) of a subspace \mathcal{S} in \mathcal{H} , written \mathcal{S}^\perp , is the set of all the

elements of \mathcal{H} orthogonal to \mathcal{S} with respect to the usual euclidean inner product. We then have $\mathcal{H} = \mathcal{S} \oplus \mathcal{S}^\perp$, the direct sum of the two orthogonal subspaces. Note that we use indifferently the notation \mathcal{K}_P or \mathcal{S}_P^\perp for a Hermitian operator P .

We need to define a positive semi-definite operator. A Hermitian operator A acting on \mathcal{H} is positive semi-definite if and only if $\langle \Psi | A | \Psi \rangle \geq 0$, for all $|\Psi\rangle$ in \mathcal{H} . In other words, a Hermitian operator is positive if and only if all its eigenvalues are positive or zero. We use the notation $A \geq 0$ to say that an operator A is positive semi-definite. For such a positive semi-definite operator A . We can define its unique square root \sqrt{A} and decompose it into the form $A = MM^\dagger$ with $M = \sqrt{A}U$, for any unitary matrix U . Since the states ρ_i and the POVM elements E_k are positive semi-definite operators, we can introduce their square root and use the previous decomposition.

1.2 Unambiguous Quantum State Discrimination

A quantum state describes what we know about a quantum system. Given a single copy of a quantum system which can be prepared in several known quantum states, our aim is to determine in which state the system is. This can be well understood in a communication context where only a single copy of the system is given and only a single shot-measurement is performed. This is in contrast with usual experiments in physics where many copies of a system are measured to get the probability distribution of the system. In quantum state discrimination (see [7] for a review of quantum state discrimination), no statistics is built since only a single-shot measurement is performed on a single copy of the system. Actually there are fundamental limitations to the precision with which the state of the system can be determined with a single measurement. Whenever the possible quantum states are nonorthogonal, perfect discrimination of the states becomes impossible. This can be understood from the intuition that two non-orthogonal states have some probability to behave the same way. More precisely, if a quantum system is prepared in one of the two state $|\Psi\rangle$ and $|\Phi\rangle$, which are neither identical nor orthogonal, there is no measurement that perfectly determines in which state the system is. Mathematically, a measurement, that perfectly determines in which state the system is, is composed of two outcomes (i.e. two POVM elements) E_Ψ and E_Φ that identify $|\Psi\rangle$ and $|\Phi\rangle$ respectively with no errors. This means, in terms of probabilities, that

$$\langle \Psi | E_\Psi | \Psi \rangle = 1, \quad (1.10)$$

$$\langle \Phi | E_\Phi | \Phi \rangle = 1, \quad (1.11)$$

$$\langle \Psi | E_\Phi | \Psi \rangle = 0, \quad (1.12)$$

$$\langle \Phi | E_\Psi | \Phi \rangle = 0. \quad (1.13)$$

If we express $|\Phi\rangle$ in the basis $\{|\Psi\rangle, |\Psi^\perp\rangle\}$, Eqn.(1.11) becomes

$$(\langle \Psi | \Phi \rangle^* \langle \Psi | + \langle \Psi^\perp | \Phi \rangle^* \langle \Psi^\perp |) E_\Phi (\langle \Psi | \Phi \rangle |\Psi\rangle + \langle \Psi^\perp | \Phi \rangle |\Psi^\perp\rangle) = 1 \quad (1.14)$$

where $*$ stands for complex conjugation. With the help of Eqn.(1.12) which is equivalent to $E_\Phi|\Psi\rangle = 0$ since $E_\Phi \geq 0$ (see proof in Appendix A), we obtain

$$|\langle\Phi|\Psi^\perp\rangle|^2\langle\Psi^\perp|E_\Phi|\Psi^\perp\rangle = 1. \quad (1.15)$$

Since the spectrum of E_Φ is upper bounded by 1, $\langle\Psi^\perp|E_\Phi|\Psi^\perp\rangle \leq 1$ and Eqn.(1.15) is fulfilled only if $|\langle\Phi|\Psi^\perp\rangle|^2 = 1$ which contradicts the assumption that $|\Psi\rangle$ and $|\Phi\rangle$ are non-orthogonal.

The immediate consequence of this limited precision is to resort to various state discrimination strategies depending on what one really wants to learn about the state. Given a strategy, we finally have to optimize the measurement with respect to some criteria.

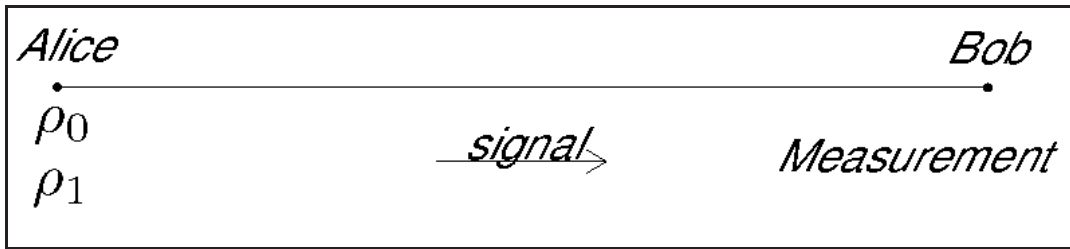


Figure 1.1: Two parties Alice and Bob want to communicate

The basic scenario involves two parties Alice and Bob who want to communicate (see Fig. 1.1). Alice prepares a quantum system in a state, member of a set of states known by Bob. In general Alice does not prepare each state with the same probability. We speak of an *a priori* probability. She sends a quantum system to Bob who performs a measurement in order to obtain the information he wants. In other words, a state ensemble of a quantum system is given and we want to determine the state of that system. In his famous book published in 1976 [3], Helstrom established the mathematical bases of such detection tasks. He introduced the notion of *Bayes' cost function* which can describe any discrimination strategy. The idea is the following. For each possible outcome k conditioned on a signal state j , a price to pay C_{kj} is associated. If C_{kj} is positive, Bob has to pay Alice. If C_{kj} is negative, Bob earns money. To set up a strategy corresponds to give the *Bayes' cost matrix* C_{kj} . Related to this matrix, the *Bayes' cost function*, given by

$$C = \sum_{kj} \eta_j C_{kj} p(k|j), \quad (1.16)$$

represents the total price that Bob has to pay to Alice. Information about a state is represented by an outcome k conditioned on a signal state j . It then appears clear that, depending on which information really matters to Bob and Alice, the strategy or, equivalently, the *Bayes' cost matrix* C_{kj} will change. The aim for Bob is of course to minimize the prize he has to pay to Alice. To

minimize the *Bayes' cost function* C while the *a priori* probability η_j and the states ρ_j are fixed, Bob is only free to change his measurement. In this thesis, we play the role of Bob who wants to find the optimal measurement to lose a minimal amount of money.

The *Bayes' cost matrix* C_{kj} depends on the strategy adopted by Alice and Bob. For instance, Bob might want to know which state was sent with the minimum error probability. This strategy is called *Minimum Error Discrimination* (MED) [3] - see Fig. 1.2. In MED, the *Bayes' cost matrix* C_{kj} is given by

$$C_{kj} = \begin{cases} 0 & k = j, \\ 1 & k \neq j. \end{cases} \quad (1.17)$$

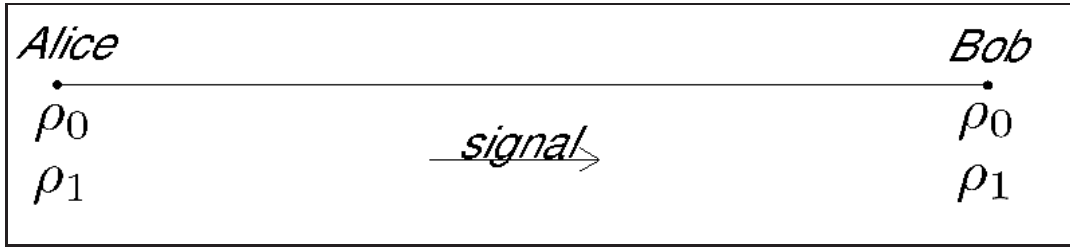


Figure 1.2: Two possible outcomes in the scenario of Minimum Error Discrimination

Alternatively, one might consider an error-free discrimination of the signal states. In this strategy, the measurement can either correctly identify the state or send out a flag stating that it failed to identify the state. A correct identification of the state is called a *conclusive result* while a failure to identify the state is known as an *inconclusive result* usually denoted by '?' or 'don't know'. The objective then is to minimize the probability of inconclusive result, the so-called *failure probability*. This strategy is called *Unambiguous State Discrimination* (USD) - see Fig. 1.3. The coefficients of the non square ($j = 0, 1$ and $k = 0, 1, ?$) are *Bayes' cost matrix* C_{kj} are

$$C_{kj} = \begin{cases} 0 & k = j, \\ 1 & k = ?, \forall j, \\ \infty & \text{otherwise.} \end{cases} \quad (1.18)$$

Note that the coefficients $C_{k \neq j}$ where $k, j = 0, 1$ are set to infinity in order to impose the error-free conditions $p(k|j \neq k) = 0, k, j = 0, 1$ to obtain a non diverging *Bayes' cost function*.

We can list another task related to state discrimination where we are given a finite number of identical copies of an unknown state in a d -dimensional Hilbert space. Our goal is to estimate the actual state with the maximum accuracy, which is often quantified by the fidelity between the actual state and the estimated state (see chapter 2 for a definition of the fidelity). Since the

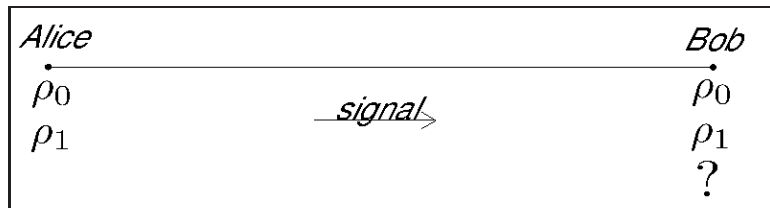


Figure 1.3: Three possible outcomes in the scenario of Unambiguous State Discrimination

state to estimate can be any state in the d -dimensional Hilbert space, one has to average the accuracy over all the possible states of the d -dimensional Hilbert space. This scenario is known as *Quantum State Estimation* [8, 9] (see Ref. [10, 11, 12] for other scenarios).

Let us add another comment. The fact that non-orthogonal quantum states are not perfectly distinguishable also has benefits. It leads in particular to secure Quantum Key Distribution (QKD) in a cryptographic context [13]. The security in classical computer science is ensured by the complexity of some task like factorization of big prime numbers. In QKD, the security is due to the quantum laws of Nature and does not anymore rely on the assumption of eavesdropper's limited computational power.

In general, the optimal measurements for a given strategy depends on the quantum states and the *a priori* probability of their appearance. For a given strategy and a given state ensemble, the task is to find the measurement which minimizes the *Bayes' cost function*. Such a measurement (it might not be unique) is called an *optimal measurement*.

In this thesis, we are interested in the unambiguous discrimination of two known mixed quantum states. Therefore the task is to find an optimal measurement that minimizes the failure probability. The problem of unambiguously discriminating pure states with equal *a priori* probabilities was formulated in 1987 by Dieks [14] and Ivanovic [15] and elegantly solved by Peres [16]. Seven years later, Jaeger and Shimony presented the general solution for two pure states with different *a priori* probabilities [17]. Shortly after this result, Chefles and Barnett showed that only linearly independent pure states can be unambiguously discriminated [18]. Finally Chefles provided the optimal failure probability and its corresponding optimal measurement in the case of n symmetric states [19]. The enumeration of analytical results for USD of pure states scenarios already ends here even if an algorithm for the case of three pure states was proposed by Peres and Terno in 1998 [20]. In fact, since Sun's work in 2002 [21, 22], it is known that USD (of both pure and mixed states) is a convex optimization problem [23, 24, 25]. Mathematically, this means that the quantity to optimize as well as the constraints on the unknowns are convex functions. Practically, this means that the optimal solution can be extremely efficiently computed. This is therefore a very useful tool. Nevertheless our aim is to

understand the structure of USD, to relate it to neat and relevant quantities and to find analytical solutions.

The case of mixed states recently attracted more attention. But until this present work, no optimal measurements for mixed states has been found unless the USD problem can be reduced to some known pure state case. This reduction comes from simple geometrical considerations and can be summarized in three theorems. Important examples of such reducible problems are *Unambiguous State Discrimination of two mixed states with one-dimensional kernel* [26], *Unambiguous State Comparison* [27, 28, 29] (see Ref. [27, 30, 31] for the unambiguous comparison of unknown states), *State Filtering* [32, 33, 34] and *Unambiguous Discrimination of two subspaces* [35]. This four cases are all reducible to some pure state case and can therefore be solved. To specify that a USD problem is not reducible by means of our three reduction theorems, we use the expression 'USD of generic density matrices'. Lower and upper bounds on the failure probability to unambiguously discriminate two density matrices are also known. In 2004, Eldar derived necessary and sufficient conditions for the optimality of a USD POVM [36]. Unfortunately these conditions appear rather difficult to solve. In contrast to the MED problem, which is already solved for any pair of mixed states [3, 37], the optimal USD of mixed states is an open problem.

1.3 Results

We outline here the six main results derived in this thesis.

- 1) **Three reduction theorems to reduce the dimension of a USD problem**
- 2) **Unambiguous comparison of n pure states with a simple symmetry**
- 3) **First class of exact solutions**
- 4) **Second class of exact solutions**
- 5) **A fourth, incomplete, reduction theorem**
- 6) **USD and BB84-type QKD protocol**

Three reduction theorems to reduce the dimension of a USD problem [Chapter 3]

As seen in the previous section, only few analytical optimal solutions in Unambiguous State Discrimination are known. For pure states scenarios, only two classes of exact solutions have been provided so far. They are the solutions for USD of two pure states [17] and USD of n linearly independent symmetric pure states [19]. In the case of mixed states, there are actually four known solutions: *unambiguous discrimination of two mixed states with one-dimensional kernel* [26], *unambiguous comparison of two pure states* [27, 28, 29], *state filtering* [32, 33, 34] and *unambiguous discrimination of two subspaces* [35]. It seems surprising that research on USD of pure states has been less successful than work on USD of mixed states! A solution to this apparent paradox is given by our first result. Indeed these four optimal solutions in USD of mixed states only require the optimal solution for USD of two pure states. More generally, we prove that the problem of discriminating any two density matrices can be reduced to the problem of discriminating two density matrices of the same rank r in a $2r$ -dimensional Hilbert space. This introduces the notion of *standard* USD problem. Such a standard USD problem is proposed as a starting point for any further theoretical investigation on USD. That way, we can avoid to deal with trivial or already known classes of solutions. The reductions are of three types and can be summarized in three theorems. In few words, the reduction theorems work as follows. In a first reduction theorem, we split off any common subspace between the supports of the two density matrices ρ_0 and ρ_1 . In a second reduction theorem, we eliminate, if present, the part of the support of ρ_1 which is orthogonal to the support of ρ_0 and *vice versa*. In a third reduction theorem, if two density matrices are block diagonal, we decompose the global USD problem into decoupled unambiguous discrimination tasks on each block.

Unambiguous comparison of n pure states with a simple symmetry [Chapter 3]

We are given n pure quantum states $\{|\Psi_i\rangle\}$ which occur with *a priori* probabilities $\{p_i\}$. We would like to know without error whether these states are all identical or not. Actually the task of unambiguously comparing any two pure states can be elegantly solved by use of the second and third reduction theorems, as Kleinmann *et al.* showed in [28]. Stimulated by their idea, we investigate the case of n pure states having some simple symmetry. In fact we prove that the comparison of n linearly independent pure states with equal *a priori* probabilities and equal and real overlaps can be reduced to n unambiguous discriminations of two pure states and then be solved. The question to know whether any unambiguous comparison of *pure* states is always reducible to some pure state cases remains opened. Let us add here that, as Kleinmann *et al.* indicated in [28], the unambiguous comparison of *mixed* states is generally not reducible to some pure states case.

In this thesis, we provide two classes of exact solutions for unambiguously discriminating two *generic* density matrices. These two classes are the only two classes known until now.

First class of exact solutions [Chapter 4]

We consider the problem of unambiguously discriminating two density matrices ρ_0 and ρ_1 with *a priori* probabilities η_0 and η_1 . We define the fidelity of the two states as $F = \text{Tr}(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}})$. We provide three lower bounds on the failure probability in three regimes of the ratio between the *a priori* probabilities defined as $\sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{\text{Tr}(P_1\rho_0)}{F}$, $\frac{\text{Tr}(P_1\rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{F}{\text{Tr}(P_0\rho_1)}$ and $\frac{F}{\text{Tr}(P_0\rho_1)} \leq \sqrt{\frac{\eta_1}{\eta_0}}$. For each regime, we give necessary and sufficient conditions for the failure probability of unambiguously discriminating two mixed states to reach the bound. With that result, we give the optimal USD POVM of a wide class of pairs of mixed states. This class corresponds to pairs of mixed states for which the lower bound on the failure probability is saturated. This is the first analytical solution for unambiguous discrimination of generic mixed states. This goes beyond known results which are all reducible to some pure state case. Note that any pair of mixed state does not saturate the bounds. The necessary and sufficient conditions take the simple form of the positivity of the two operators $\rho_0 - \alpha\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\rho_1 - \frac{1}{\alpha}\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$ where α equals $\frac{\text{Tr}(P_1\rho_0)}{F}$, $\sqrt{\frac{\eta_1}{\eta_0}}$ and $\frac{F}{\text{Tr}(P_0\rho_1)}$ in the first, second and third regime, respectively.

Second class of exact solutions [Chapter 5]

We derive a second class of exact solutions. This class corresponds to any pair of *geometrically uniform* mixed states without overlapping supports in a four dimensional Hilbert space. In short, two *geometrically uniform* mixed states are two unitary similar density matrices ρ_0 and $\rho_1 = U\rho_0U$ where the unitary matrix U is an involution i.e. $U^2 = \mathbb{1}$. We find that only three options for the expression of the failure probability exist. First, if the operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1$ are positive semi-definite, then the pair of density matrices falls in the first class of exact solutions. If this is not the case, either the operator $P_0^\perp U P_0^\perp$ has one positive and one negative eigenvalue or it has two eigenvalues of the same sign. In the former case, we can give the optimal failure probability in terms of the eigenvalues and eigenvectors of $P_0^\perp U P_0^\perp$. In the later case, no unambiguous discrimination is possible and the failure probability simply equals unity. For these three cases, we provide the optimal failure probability as well as the optimal measurement.

A fourth, incomplete, reduction theorem [Chapter 5]

The two USD POVM elements E_0 and E_1 have a rank less or equal to the rank of $\mathcal{S}_{\rho_1}^\perp$ and $\mathcal{S}_{\rho_0}^\perp$, respectively. This defines the notion of maximum rank of E_0 and E_1 . We establish a theorem stating that if the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1$ are not positive semi-definite then the two USD POVM elements E_0 and E_1 can not have both maximum rank. A corollary can be derived assuming a standard USD problem. In that case, if the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1$ are not positive semi-definite then there exist one eigenvector of

$E_?$ with eigenvalue 1 and one eigenvector of either E_0 or E_1 with eigenvalue 1, too. From the completeness relation fulfilled by the measurement operators, it follows that we can split off the two-dimensional subspace spanned by these two eigenvectors from the original USD problem. This could lead to a fourth reduction theorem. 'Could' because it remains to fully characterize these two eigenvectors cited above. So far, we can only prove their existence. If one could characterize them, a way to solve analytically any USD problem would be available. Indeed, we start from a general USD problem of two mixed states. We use the three first reduction theorems to bring it to standard form. We then check the positivity of the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1$. If the positivity is confirmed, then the pair of density matrices falls in the first class of exact solutions. If the two operators are not positive, we can use the fourth reduction theorem to get rid of two dimensions corresponding to the two eigenvectors mentioned above. At that point, we check the positivity of the two operators $\rho'_0 - \sqrt{\frac{\eta'_1}{\eta'_0}} F'_0$ and $\rho'_1 - \sqrt{\frac{\eta'_0}{\eta'_1}} F'_1$ of the reduced problem. We see here a constructive way to solve any USD problem. If the two operators $\rho'_0 - \sqrt{\frac{\eta'_1}{\eta'_0}} F'_0$ and $\rho'_1 - \sqrt{\frac{\eta'_0}{\eta'_1}} F'_1$ of the reduced problems never turn out to be positive, we end up with only two pure states and we can therefore always find the optimal measurement. The full characterization of the two eigenvectors involved in this incomplete reduction theorem is of great importance.

USD and BB84-type QKD protocol [Chapter 6]

The Bennett and Brassard 1984 cryptographic protocol [38] provides a method to distribute a private key between two parties and allow an unconditionally secure communication. We consider in this thesis the implementation of a BB84-type QKD protocol that uses weak coherent pulses with a phase reference [39]. In that context, two important questions related to unambiguous state discrimination can be addressed. First, 'With what probability can an eavesdropper unambiguously distinguish the *basis* of the signal?' and second 'With what probability can an eavesdropper unambiguously determine which *bit value* is sent without being interested in the knowledge of the basis?' These two questions can be translated in some unambiguous discrimination task of two *geometrically uniform* mixed states in a four dimensional Hilbert space. We answer these two questions providing useful insights for further investigations on practical implementations of Quantum Key Distribution protocols.

The structure of this thesis is the following. In chapter 2, we mathematically define the problem of USD. We then review the known results on unambiguous discrimination: unambiguous discrimination two pure states, unambiguous discrimination of n symmetric states and a few general properties. In chapter 3, we present our three reduction theorems. They allow us to solve special tasks in quantum information theory such as, e.g. state filtering, unambiguous discrimi-

nation of two pure states, unambiguous discrimination of n pure states with a simple symmetry and unambiguous discrimination of two subspaces. All these tasks are related to the unambiguous discrimination of two mixed states which can be reduced to the unambiguous discrimination of some pure states only. We also define a *standard* form as a starting point for further investigations in USD. In chapter 4, we derive lower bounds on the failure probability Q as well as necessary and sufficient conditions for the failure probability to reach those bounds. This provides a first class of exact solutions for unambiguous discrimination of two *generic* mixed states. This class corresponds to pairs of mixed states for which the lower bound (one for each of the three regimes depending on the ratio between the *a priori* probabilities) on the failure probability Q is saturated. For this class we give the corresponding optimal USD measurement. In chapter 5, we derive a fourth, incomplete, reduction theorem which, together with the first three reduction theorems aims to solve in a constructive way any USD problem of two density matrices. Moreover we derive a second class of exact solutions. This class corresponds to any pair of two geometrically uniform states in four dimensions. In chapter 6, we give two examples of such an unambiguous discrimination of two *geometrically uniform* states in four dimensions. These examples are related to the implementation of the Bennett and Brassard 1984 cryptographic protocol. In the last chapter, we summarize our results and propose directions for further research on USD of two density matrices.

Chapter 2

Optimal Unambiguous State Discrimination

The optimal USD measurement is known for two *pure-state* cases. On one hand, the optimal failure probability as well as the corresponding optimal measurement were provided by Jaeger and Shimony for any pair of two pure states with arbitrary *a priori* probabilities [17]. On the other hand, Chefles found the optimal failure probability and the corresponding optimal measurement for unambiguously discriminating n linearly independent symmetric pure states [19]. We present the basic properties of a USD measurement before reviewing the solution to these two *pure-state* scenarios.

2.1 The USD measurement

We consider a set of $n \in \mathbb{N}$ known quantum states $\{\rho_i\}$, $i = 1, \dots, n$, with their *a priori* probabilities $\{\eta_i\}$. We are looking for a measurement that either identifies a state uniquely (conclusive result) or fails to identify it (inconclusive result). The goal is to minimize the probability of inconclusive result. The measurements involved are typically generalized measurements [2] described by a POVM which consists in a set of positive semi-definite operators $\{E_k\}$ that satisfies the completeness relation $\sum_k E_k = \mathbb{1}$ on the Hilbert space spanned by the states. The probability to obtain the outcome k for a given signal ρ_i is then given by $p(k|i) = \text{Tr}(\rho_i E_k)$. We will often refer to the states of the quantum system as *signal* states or even *signals*. This comes from the context of communication where the possible states of a quantum system correspond to the different signals sent to communicate.

Let us now mathematically define what an Unambiguous State Discrimination Measurement is, its corresponding failure probability, and the notion of optimality.

Definition 3 A measurement described by a POVM $\{E_k\}$ is called an *Unambiguous State Discrimination Measurement (USD)* on a set of states $\{\rho_i\}$ if and only if the following conditions are satisfied:

- The POVM contains the elements $\{E_?, E_1, \dots, E_n\}$ where n is the number of different signals in the set of states. The element $E_?$ is connected to an inconclusive result, while the other elements E_i , $i = 1, \dots, n$, correspond to an identification of the state ρ_i .
- No states are wrongly identified, that is $\text{Tr}(\rho_i E_k) = 0 \quad \forall i \neq k \quad i, k = 1, \dots, n$.

Each USD Measurement gives rise to a failure probability, that is, the rate of inconclusive results. This can be calculated as

$$Q[\{E_k\}] := \sum_i \eta_i \text{Tr}(\rho_i E_?). \quad (2.1)$$

Definition 4 A measurement described by a POVM $\{E_k^{opt}\}$ is called an *Optimal Unambiguous State Discrimination Measurement (OptUSD)* on a set of states $\{\rho_i\}$ with the corresponding a priori probabilities $\{\eta_i\}$ if and only if the following conditions are satisfied

- The POVM $\{E_k^{opt}\}$ is a USD measurement on $\{\rho_i\}$
- The probability of inconclusive results is minimal, that is $Q[\{E_k^{opt}\}] = \min Q[\{E_k\}]$ where the minimum is taken over all USD.

Unambiguous state discrimination is an error-free discrimination. This implies a strong constraint on the measurement. The fact that the outcome E_k can only be triggered by the state ρ_k implies that the support of E_k is orthogonal to the supports of all the mixed states other than ρ_k . This is a strong constraint for any USD measurement, not only the optimal one. To see that fact rigorously we need the following lemma.

Lemma 1 For any positive semi-definite operators A and B , $\text{Tr}(AB) = 0$ if and only if the support of the two positive semi-definite operators are orthogonal

$$\text{Tr}(AB) = 0 \Leftrightarrow S_A \perp S_B. \quad (2.2)$$

Since a USD POVM satisfies $\text{Tr}(E_k \rho_i) = \text{Tr}(E_k \rho_k) \delta_{ki}$ to be an error-free measurement, a corollary of Lemma 1 can be derived.

Corollary 2 A USD measurement described by the POVM $\{E_k\}$ on n density matrices $\{\rho_i\}$ is such that

$$S_{E_k} \perp S_{\rho_{i \neq k}}, \quad \forall i, k = 1, \dots, n. \quad (2.3)$$

USD measurements are very sensitive in the sense that a small variation of a mixed state overthrows completely the error-free character of the already existing measurement. This is true for any USD measurement, not only the optimal ones. Let us now prove Lemma 1.

Proof of Lemma 1 If A and B are positive semi-definite operators, they are diagonalizable with eigenvalues $\alpha_i > 0$ ($i = 1, \dots, \text{rank}(A)$) and $\beta_j > 0$ ($j = 1, \dots, \text{rank}(B)$). Thus

$$\begin{aligned} \text{Tr}(AB) &= \text{Tr}\left(\sum_i \alpha_i |\Psi_i\rangle\langle\Psi_i| \sum_j \beta_j |\Phi_j\rangle\langle\Phi_j|\right) \\ &= \sum_{ij} \alpha_i \beta_j |\langle\Psi_i|\Phi_j\rangle|^2 \end{aligned} \quad (2.4)$$

vanishes if and only if $\{|\Phi_i\rangle\}$ and $\{|\Psi_j\rangle\}$ span orthogonal subspaces. ■

2.2 Solution for two pure states

In the simple case of two pure states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ with arbitrary *a priori* probabilities η_0 and η_1 , the optimal failure probabilities (see Fig. 2.1) to unambiguously discriminate them is given by

$$Q^{\text{opt}} = \eta_1 + \eta_0 |\langle\Psi_0|\Psi_1\rangle|^2 \text{ for } \sqrt{\frac{\eta_1}{\eta_0}} \leq |\langle\Psi_0|\Psi_1\rangle|, \quad (2.5)$$

$$Q^{\text{opt}} = 2\sqrt{\eta_0\eta_1} |\langle\Psi_0|\Psi_1\rangle| \text{ for } |\langle\Psi_0|\Psi_1\rangle| \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{|\langle\Psi_0|\Psi_1\rangle|}, \quad (2.6)$$

$$Q^{\text{opt}} = \eta_0 + \eta_1 |\langle\Psi_0|\Psi_1\rangle|^2 \text{ for } \frac{1}{|\langle\Psi_0|\Psi_1\rangle|} \leq \sqrt{\frac{\eta_1}{\eta_0}}. \quad (2.7)$$

This result was derived by Jaeger and Shimony in 1995. When the two *a priori* probabilities are equal, it reduces to the well known equation

$$Q^{\text{opt}} = |\langle\Psi_0|\Psi_1\rangle|. \quad (2.8)$$

This solution is known as the Ivanovic-Diesk-Peres (IDP) limit since 1988.

The optimal measurement (see Fig. 2.2) that realizes these optimal failure probabilities is given by

$$\begin{aligned} E_0 &= |\Psi_1^\perp\rangle\langle\Psi_1^\perp| \\ E_1 &= 0 \\ E_? &= |\Psi_1\rangle\langle\Psi_1| \end{aligned} \text{ for } \sqrt{\frac{\eta_1}{\eta_0}} \leq |\langle\Psi_0|\Psi_1\rangle|, \quad (2.9)$$

$$\begin{aligned} E_0 &= \frac{1 - \sqrt{\frac{\eta_1}{\eta_0}} |\langle\Psi_0|\Psi_1\rangle|}{|\langle\Psi_1^\perp|\Psi_0\rangle|^2} |\Psi_1^\perp\rangle\langle\Psi_1^\perp| \\ E_1 &= \frac{1 - \sqrt{\frac{\eta_0}{\eta_1}} |\langle\Psi_0|\Psi_1\rangle|}{|\langle\Psi_0^\perp|\Psi_1\rangle|^2} |\Psi_0^\perp\rangle\langle\Psi_0^\perp| \\ E_? &= \mathbb{1} - E_0 - E_1 \end{aligned} \text{ for } |\langle\Psi_0|\Psi_1\rangle| \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{|\langle\Psi_0|\Psi_1\rangle|}, \quad (2.10)$$

$$\begin{aligned}
E_0 &= 0 \\
E_1 &= |\Psi_0^\perp\rangle\langle\Psi_0^\perp| \text{ for } \frac{1}{|\langle\Psi_0|\Psi_1\rangle|} \leq \sqrt{\frac{\eta_1}{\eta_0}} \\
E_2 &= |\Psi_0\rangle\langle\Psi_0|
\end{aligned} \tag{2.11}$$

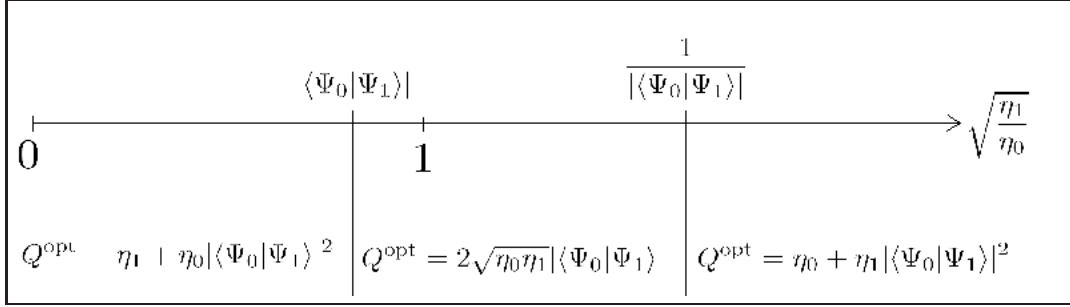


Figure 2.1: Optimal failure probability for USD of two pure states

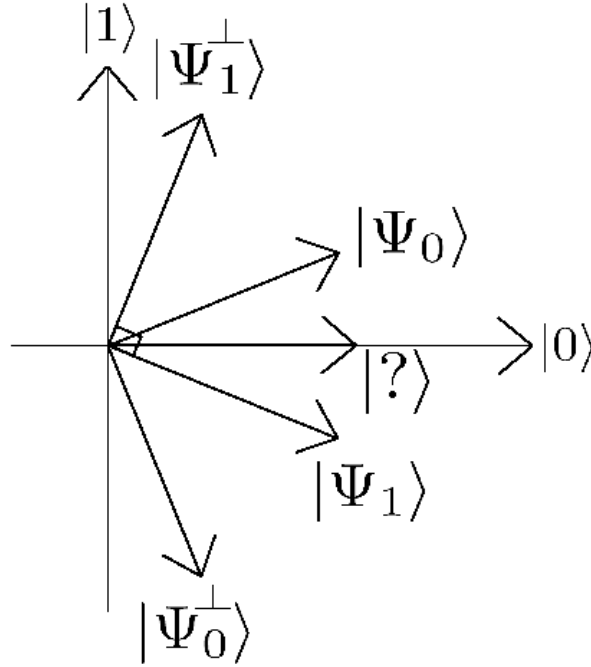


Figure 2.2: Basis vectors $|\Psi_1^\perp\rangle$, $|\Psi_0^\perp\rangle$ and $|?\rangle$ of the three POVM elements E_0 , E_1 and E_2 for the optimal USD measurement of two pure states when $\langle\Psi_0|\Psi_1\rangle \geq 0$ and $|\langle\Psi_0|\Psi_1\rangle| \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{|\langle\Psi_0|\Psi_1\rangle|}$

2.3 Solution for n symmetric pure states

Unambiguous discrimination can be considered for more than two states. The only requirement for an error-free discrimination is the linear independence of the signal states as Chefles showed in 1998. An exact solution can even be provided if the n quantum states happen to be symmetric. Symmetric states are states that can be written in terms of a generator $|\Psi_0\rangle$ and a unitary transformation U such that $U^n = \mathbb{1}$. The complete set of symmetric states can be written as

$$|\Psi_j\rangle = U|\Psi_{j-1}\rangle = U^j|\Psi_0\rangle, \quad j = 1, \dots, n-1 \quad (2.12)$$

$$|\Psi_0\rangle = U|\Psi_{n-1}\rangle, \quad U^n = \mathbb{1}. \quad (2.13)$$

Note that we choose the *a priori* probabilities to be equal in order not to break the symmetry. For such symmetric states, we can introduce a suitable orthonormal basis $\{|\gamma_k\rangle\}_k$ such that $|\Psi_j\rangle = \sum_{k=0}^{n-1} c_k e^{2i\pi \frac{jk}{n}} |\gamma_k\rangle$ with $\sum_k |c_k|^2 = 1$ and $U = \sum_{k=0}^{n-1} e^{2i\pi \frac{k}{n}} |\gamma_k\rangle\langle\gamma_k|$ [19]. Note that the coefficients c_k can be calculated thanks to the formula $|c_k|^2 = \frac{1}{n^2} \sum_{j,j'} e^{2i\pi k \frac{j-j'}{n}} \langle\Psi_{j'}|\Psi_j\rangle$. We define $c_{\min} = \min_k c_k$ and the optimal failure probabilities to unambiguously discriminate n symmetric states is then given by

$$Q^{\text{opt}} = n|c_{\min}|^2. \quad (2.14)$$

On the analytical side, some general properties of USD of mixed states were recently derived. We give here an overview of these results. First, there are the very general necessary and sufficient conditions for the optimality of a USD measurement derived by Eldar in [36]. Unfortunately those conditions are pretty hard to solve. They can nevertheless be used to check the optimality of some USD POVM or, as we will do in chapter 5, to derive a new class of exact solutions. This class corresponds to pairs of two Geometrically Uniform density matrices in four dimensions. Another general result on USD of two mixed states is the derivation of lower and upper bounds on the optimal failure probability. The lower bounds are expressed in terms of the fidelity. Therefore we first introduce this quantity. The upper bound is presented in terms of the failure probabilities of some pure state case.

2.4 Necessary and sufficient conditions for the optimality of a USD measurement

Necessary and sufficient conditions for an optimal measurement that minimizes the probability of inconclusive result can be derived using argument of duality in vector space optimization [36]. These conditions are valid for any number of mixed states. Let us now state the theorem.

Theorem 3 Let $\{\rho_i\}$, $1 \leq i \leq n$ denote a set of density operators with their *a priori* probabilities $\{\eta_i\}$. Let denote T_i and Δ_i two matrices such that $E_i = T_i \Delta_i T_i^\dagger$, $\Delta_i \geq 0$ and $T_i T_i^\dagger = \Pi_{\mathcal{S}_{E_i}}$, the

projection onto the support of E_i , for all $1 \leq i \leq n$. Then necessary and sufficient conditions for a measurement $\{E_k\}$, $k=0,1,\dots,n$ to be an optimal USD measurement are that there exists $Z \geq 0$ such that

$$ZE_? = 0 \quad (2.15)$$

$$E_i(Z - \eta_i \rho_i)E_i = 0, \quad 1 \leq i \leq n \quad (2.16)$$

$$T_i^\perp(Z - \eta_i \rho_i)T_i^\perp \geq 0, \quad 1 \leq i \leq n \quad (2.17)$$

We could rephrase this theorem for two mixed states only. The statement then is slightly simpler.

Theorem 4 Let ρ_0 and ρ_1 be two density matrices with a priori probabilities η_0 and η_1 . We denote by P_0^\perp and P_1^\perp , the projectors onto the kernel of ρ_0 and ρ_1 . Then necessary and sufficient conditions for an optimal measurement $\{E_k\}$, $k=0,1$ are that there exists $Z \geq 0$ such that

$$ZE_? = 0, \quad (2.18)$$

$$E_0(Z - \eta_0 \rho_0)E_0 = 0, \quad (2.19)$$

$$E_1(Z - \eta_1 \rho_1)E_1 = 0, \quad (2.20)$$

$$P_1^\perp(Z - \eta_0 \rho_0)P_1^\perp \geq 0, \quad (2.21)$$

$$P_0^\perp(Z - \eta_1 \rho_1)P_0^\perp \geq 0 \quad (2.22)$$

One could try to find the general solution for unambiguously discriminating two mixed states by solving the above conditions. However, in the general case it appears difficult to find a positive semi-definite operator Z fulfilling those conditions. Before ending this section, we can notice that

$$\text{Tr}(Z) = P_{\text{success}}^{\text{opt}}. \quad (2.23)$$

Indeed Eqn.(2.19) is equivalent to $\sqrt{E_0}(Z - \eta_1 \rho_1)\sqrt{E_0} = 0$. Its trace leads to $\text{Tr}(ZE_0) = \eta_0 \text{Tr}(\rho_0 E_0)$. Similarly Eqn.(2.20) yields $\text{Tr}(ZE_1) = \eta_1 \text{Tr}(\rho_1 E_1)$ so that $\text{Tr}(ZE_0) + \text{Tr}(ZE_1) = P_{\text{success}}^{\text{opt}}$. The completeness relation $\mathbb{1} = E_? + E_0 + E_1$ together with Eqn.(2.18) gives $\text{Tr}(Z) = P_{\text{success}}^{\text{opt}}$. Later in this thesis, we will use Eldar's necessary and sufficient conditions to derive a theorem about the rank of the POVM elements of an optimal USD measurement and a new class of exact solutions of USD.

2.5 Bounds on the failure probability

2.5.1 Fidelity

The fidelity $F(\rho_0, \rho_1) = \text{Tr}(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}})$ is a quantity to distinguish two mixed quantum states ρ_0 and ρ_1 .

We can consider the two extreme cases $\rho_0 = \rho_1$ and $\mathcal{S}_{\rho_0} \perp \mathcal{S}_{\rho_1}$. On one hand, if $\rho_0 = \rho_1$ then $F(\rho_0, \rho_1) = 1$. On the other hand, if ρ_0 and ρ_1 have orthogonal supports then $F(\rho_0, \rho_1) = 0$. The fidelity takes value in $[0, 1]$. when $F = 1$, the two states are identical. When $F = 0$, the two states have orthogonal supports. It is not obvious that the fidelity is a symmetric quantity in its two arguments, though it is as we will show here [40, 41]. We can first consider the fidelity of two pure states.

$$\begin{aligned} F(|\Psi_0\rangle\langle\Psi_0|, |\Psi_1\rangle\langle\Psi_1|) &= \text{Tr}(\sqrt{|\Psi_0\rangle\langle\Psi_0||\Psi_1\rangle\langle\Psi_1||\Psi_0\rangle\langle\Psi_0|}) \\ &= |\langle\Psi_0|\Psi_1\rangle| \text{Tr}(\sqrt{|\Psi_1\rangle\langle\Psi_1|}) \\ &= |\langle\Psi_0|\Psi_1\rangle|. \end{aligned} \quad (2.24)$$

The fidelity of two pure states simply is the modulus of the overlap between those two pure states! The fidelity is here clearly symmetric. If we now consider mixed states, we can define the operators $F_0 = \sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $F_1 = \sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. They actually come from the polar decomposition

$$\sqrt{\rho_0}\sqrt{\rho_1} = F_0V = VF_1. \quad (2.25)$$

As written in Eqn.(2.25), the two operators F_0 and F_1 are unitary equivalent and their trace are equal. In other words,

$$F(\rho_i, \rho_j) = \text{Tr}(F_i) = \text{Tr}(F_j) \quad (2.26)$$

and the fidelity is symmetric. It might be sometimes difficult to work with the fidelity because of the three square roots involved in its definition and because of the noncommutativity of the density operators. For a review of its properties, the interested reader should look at Jozsa's 1994 paper [40] inspired by Uhlmann's *transition probability* [41]. Let us however note here that in our work, the fidelity is given by $F(\rho_i, \rho_j) = \text{Tr}(\sqrt{\sqrt{\rho_i}\rho_j\sqrt{\rho_i}})$ and not by $F(\rho_i, \rho_j) = \{\text{Tr}(\sqrt{\sqrt{\rho_i}\rho_j\sqrt{\rho_i}})\}^2$ [40] though the properties remain intact.

Actually one can construct a distance measure from the fidelity, the *Bures* distance $d_{\text{Bures}}^2(\rho_i, \rho_j) = 2(1 - F(\rho_i, \rho_j))$. It is well known that the problem of minimum error discrimination between two mixed states is linked to the *trace* distance as $P_{\text{error}} = \frac{1}{2}(1 - \text{Tr}(|\eta_0\rho_0 - \eta_1\rho_1|))$. As we are going to see through this thesis, a link between Fidelity and the failure probability Q in USD does exist. It is not as strong as the link between the *trace* distance as the error probability P_{error} in MED. In chapter 4, 5 and 6, we will intensively use the fidelity.

2.5.2 Lower bound for the unambiguous discrimination of n mixed states

Y. Feng *et al.* obtained a very general lower bound for unambiguously discriminating n mixed states $\{\rho_i\}$ with *a priori* probabilities $\{\eta_i\}$ [42].

Theorem 5 Let $\{\rho_i\}$ be n density matrices with their a priori probabilities η_i . We define the fidelity of two states ρ_i and ρ_j as $F(\rho_i, \rho_j) = \text{Tr}(\sqrt{\sqrt{\rho_i}\rho_j\sqrt{\rho_i}})$. Then, for any USD measurement a lower bound on the failure probability Q is

$$Q \geq \sqrt{\frac{n}{n-1} \sum_{i \neq j}^n \eta_i \eta_j F^2(\rho_i, \rho_j)}. \quad (2.27)$$

Let us note here that another lower bound on the failure probability was derived by Y. Feng *et al.* (two of the three authors of Ref. [42]) in an unpublished work [43]. Let us notice that this bound is given as an upper bound on the success probability.

Theorem 6 Let $\{\rho_i\}$ be n density matrices with their a priori probabilities $\{\eta_i\}$. First we define the subspace $\text{Mix}(\rho_i)$ as $\text{Mix}(\rho_i) = \mathcal{S}_{\rho_i} \cap \sum_{j \neq i} \mathcal{S}_{\rho_j}$. Second, we divide each ρ_i in two parts, $\tilde{\rho}_i$ and $\hat{\rho}_i$ such that $\mathcal{S}_{\tilde{\rho}_i} = \text{Mix}(\rho_i)$ and $\mathcal{S}_{\tilde{\rho}_i} \cap \mathcal{S}_{\hat{\rho}_i} = 0$. Finally we define the fidelity of two states ρ_i and ρ_j as $F(\rho_i, \rho_j) = \text{Tr}(\sqrt{\sqrt{\rho_i}\rho_j\sqrt{\rho_i}})$. Then, for any USD measurement an upper bound on the success probability P_{success} is

$$P_{\text{success}} \leq \sum_{i=1}^n \eta_i \text{Tr}(\tilde{\rho}_i) - \sqrt{\frac{n}{n-1} \sum_{i \neq j}^n \eta_i \eta_j F^2(\tilde{\rho}_i, \tilde{\rho}_j)}. \quad (2.28)$$

This last bound is tighter than the one in Theorem 5 since $\sum_{i=1}^n \eta_i \text{Tr}(\tilde{\rho}_i) \leq 1$. The equality holds only if the density matrices ρ_i do not have common subspaces. In that case, the two lower bounds in Eqn.(2.27) and Eqn.(2.28) are equal. We now focus on USD of two density matrices only. Rudolph *et al.* derived both lower and upper bounds on the failure probability to unambiguously discriminate two mixed states. This is the object of the last subsection of this chapter.

2.5.3 Lower and upper bounds on the failure probability for the unambiguous discrimination of two mixed states

Lower bound

In Ref.[26], Rudolph *et al.* derived their lower bounds considering some purification of the two mixed states ρ_0 and ρ_1 . Moreover, an interesting property of the fidelity is the following. Given two mixed states, we can consider all their possible purification and their overlap. In fact, the fidelity equals the maximum of the modulus of those overlaps. It is therefore not surprising that those lower bounds involve the optimal failure probability of two pure states where the overlap is replaced by the Fidelity (see Fig. 2.3). More precisely, we end up with

Theorem 7 Let ρ_0 and ρ_1 be two density matrices with a priori probabilities η_0 and η_1 . Let define the fidelity $F = \text{Tr}(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}})$ between these two mixed states. Then a lower bound

on the failure probability of unambiguously discriminating ρ_0 and ρ_1 is

$$Q^{\text{opt}} \geq \eta_1 + \eta_0 F^2 \text{ for } \sqrt{\frac{\eta_1}{\eta_0}} \leq F, \quad (2.29)$$

$$Q^{\text{opt}} \geq 2\sqrt{\eta_0 \eta_1} F \text{ for } F \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{F}, \quad (2.30)$$

$$Q^{\text{opt}} \geq \eta_0 + \eta_1 F^2 \text{ for } \frac{1}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}}. \quad (2.31)$$

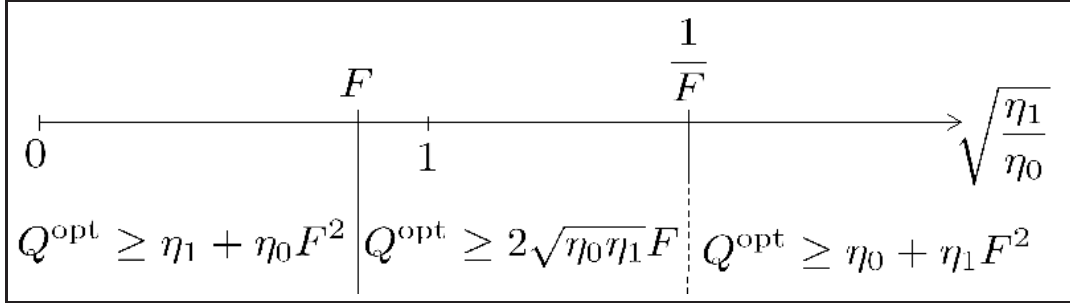


Figure 2.3: Lower bounds on the optimal failure probability for USD of two density matrices

Upper bound

In the same paper [26], the authors presented an upper bound on the optimal failure probability for unambiguous discrimination of two mixed states. This bound comes from considering several two dimensional USD problems rather than a global USD problem. The eigenbases for E_0 and E_1 here depend only on the supports of ρ_0 and ρ_1 and not on their eigenvalues. This leads naturally to an upper bound on the failure probability since the eigenvalues of ρ_0 and ρ_1 would allow to refine the measurement. The theorem presents a lower bound on the success probability instead of an upper bound on the failure probability.

Theorem 8 Let ρ_0 and ρ_1 be two density matrices with a priori probabilities η_0 and η_1 . We denote the dimension of their kernel \mathcal{K}_0 and \mathcal{K}_1 by s_0 and s_1 and assume that $s_0 \geq s_1$. There exist orthonormal bases $\{|k_b^j\rangle\}_{j=1}^{s_b}$ for \mathcal{K}_b ($b=0,1$) such that for $1 \leq j \leq s_0$, $1 \leq i \leq s_1$,

$$\langle k_0^j | k_1^i \rangle = \cos(\theta_j) \delta_{ij}, \quad (2.32)$$

where the θ_j are the canonical angles between \mathcal{K}_0 and \mathcal{K}_1 . In this case, a lower bound on the optimal success probability $P_{\text{success}}^{\text{opt}}$ is

$$P_{\text{success}}^{\text{opt}} \geq \sum_{j=1}^{s_1} P_{\text{success}}^{\text{opt}}(|k_0^j\rangle, |k_1^j\rangle) + \sum_{j=s_1+1}^{s_0} \langle k_0^j | \rho_1 | k_0^j \rangle. \quad (2.33)$$

where

$$P_{success}^{opt}(|k_0^j\rangle, |k_1^j\rangle) = \begin{cases} A_0^j + A_1^j - 2\cos(\theta_j)\sqrt{A_0^j A_1^j} & \text{for } \cos(\theta_j) < \sqrt{\frac{A_{min}^j}{A_{max}^j}} \\ A_{max}^j & \text{otherwise} \end{cases} \quad (2.34)$$

with $A_0^j = \eta_0 \langle k_1^j | \rho_0 | k_1^j \rangle$, $A_1^j = \eta_1 \langle k_0^j | \rho_1 | k_0^j \rangle$, $A_{min}^j = \min\{A_0^j, A_1^j\}$ and $A_{max}^j = \max\{A_0^j, A_1^j\}$.

Let us note that we will detail the construction of such orthogonal bases $\{|k_b^j\rangle\}_{j=1}^{s_b}$ in Chapter 3 when we will present the optimal unambiguous discrimination of two subspaces.

In the next chapter, we will find that any USD problem can be reduced to some standard situation. We will then see that some important tasks in Quantum Information Theory which are related to the USD of some mixed states can actually be reduced to some pure state case.

Chapter 3

A standard form

We are searching for an optimal USD measurement to discriminate two arbitrary density matrices ρ_0 and ρ_1 with *a priori* probability η_0 and η_1 respectively. We find that this general problem can be reduced to a simpler standard situation thanks to three *reduction* theorems dealing with simple geometrical considerations. As their names indicate, the three *reduction* theorems allow to reduce the dimension of the USD problem. In fact, the reduction can also be applied to the case of more than two density matrices.

It is important to notice here that all the results on USD of mixed states known so far are reducible to some pure state scenarios. These cases are state filtering, unambiguous discrimination of two subspaces and unambiguous comparison of two pure states. Those three cases of USD of mixed states can be solved using some reduction theorem and the result of Jaeger and Shimony about USD of two pure states only. This underlines the fact that those cases were solved first because no new techniques were needed. In the following we will often refer to *non-reducible* mixed state case as generic USD problem. In the next chapters we are going to present two classes of exact solutions for such generic USD problems. But first of all, let us present, prove and use the three reduction theorems.

The first reduction theorem states that, if two density matrices share a common subspace (see Fig. 3.1), no unambiguous discrimination is possible on it. Indeed any state vector in such a common subspace belongs to both ρ_0 and ρ_1 so that no conclusive result is possible. The failure probability restricted to this common subspace then equals unity. There is no optimization to perform onto this common subspace and we can focus our attention on the USD problem onto the orthogonal complement of this common subspace.

The second theorem is easy to understand, though the proof happens to be subtle. Let us consider the support \mathcal{S}_{ρ_0} and \mathcal{S}_{ρ_1} of two density matrices. Let us assume that there exists a subspace of \mathcal{S}_{ρ_1} orthogonal to \mathcal{S}_{ρ_0} (see Fig. 3.2). This subspace can be equivalently denoted by

$\mathcal{S}_{\rho_1} \cap \mathcal{S}_{\rho_0}^\perp$ or $\mathcal{S}_{\rho_1} \cap \mathcal{K}_{\rho_0}$. If we perform any measurement on that subspace, we can only detect ρ_1 but never ρ_0 since the measurement is orthogonal to \mathcal{S}_{ρ_0} . The difficulty step is to see that such a strategy is optimal. Here again, no optimization onto the subspace $\mathcal{S}_{\rho_1} \cap \mathcal{K}_{\rho_0}$ is needed. After splitting off $\mathcal{S}_{\rho_1} \cap \mathcal{K}_{\rho_0}$, we are left with a smaller USD problem. Of course, a similar reduction can be performed for the subspace $\mathcal{S}_{\rho_0} \cap \mathcal{K}_{\rho_1}$.

The last theorem refers to some block diagonal structure of the supports \mathcal{S}_{ρ_0} and \mathcal{S}_{ρ_1} of our two density matrices ρ_0 and ρ_1 . If the supports \mathcal{S}_{ρ_0} and \mathcal{S}_{ρ_1} can be simultaneously decomposed into a direct sum of some subspaces, it seems reasonable that the optimal measurement can have the same property. Moreover we can choose the optimal measurement onto the total Hilbert space to be the direct sum of optimal measurements onto the smaller subspaces. In other words, we only have to look for optimality on each orthogonal subspace. This again simplifies the optimization task.

Let us now derive the three theorems.

3.1 Overlapping supports

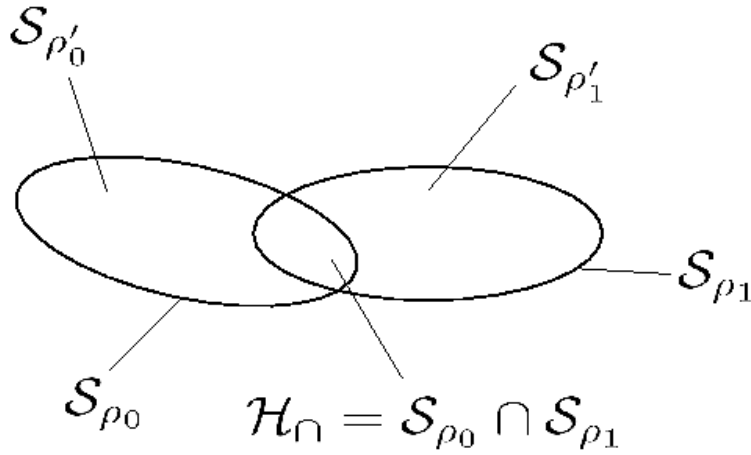
In the first theorem, we will consider the situation where the supports of the two density matrices have a common subspace. This is the case whenever we find that

$$\dim(\mathcal{S}_{\rho_0}) + \dim(\mathcal{S}_{\rho_1}) > \dim(\mathcal{H}). \quad (3.1)$$

Here \mathcal{H} is the Hilbert space spanned by the two supports. In this case, it can be written as

$$\mathcal{H} = \mathcal{H}' \oplus \mathcal{H}_\cap \quad (3.2)$$

where $\mathcal{H}_\cap = \mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1}$ is the common subspace of the two supports, and \mathcal{H}' , its orthogonal complement in \mathcal{H} (see Fig. 3.1). The first reduction theorem will eliminate the common subspace \mathcal{H}_\cap from the problem. The intuitive reason is that in this subspace no unambiguous discrimination is possible, so the population of the two density matrices on it will contribute always only to the failure probability, never to the conclusive results. This is made precise in the following theorem.

Figure 3.1: Illustration of a common subspace between ρ_0 and ρ_1 **Theorem 9** *Reduction Theorem for a Common Subspace*

Suppose we are given two density matrices ρ_0 and ρ_1 in \mathcal{H} with a priori probabilities η_0 and η_1 such that their respective supports \mathcal{S}_{ρ_0} and \mathcal{S}_{ρ_1} have a non-empty common subspace \mathcal{H}_{\cap} . We denote by \mathcal{H}' the orthogonal complement of \mathcal{H}_{\cap} in \mathcal{H} while $\Pi_{\mathcal{H}_{\cap}}$ and $\Pi_{\mathcal{H}'}$ denote respectively the projector onto \mathcal{H}_{\cap} and \mathcal{H}' . Then the optimal USD measurement is characterized by POVM elements of the form

$$E_0^{opt} = E_0'^{opt} \quad (3.3)$$

$$E_1^{opt} = E_1'^{opt} \quad (3.4)$$

$$E_{?}^{opt} = E_{?}'^{opt} + \Pi_{\mathcal{H}_{\cap}} \quad (3.5)$$

where the operators $E_0'^{opt}, E_1'^{opt}, E_{?}'^{opt}$ form a POVM $\{E_k'^{opt}\}$ with support on \mathcal{H}' describing the OptUSDM of a reduced problem defined by

$$\rho'_0 = \frac{1}{N_0} \Pi_{\mathcal{H}'} \rho_0 \Pi_{\mathcal{H}'}, \quad \eta'_0 = \frac{N_0 \eta_0}{N}, \quad N_0 = \text{Tr}(\rho_0 \Pi_{\mathcal{H}'}) \quad (3.6)$$

$$\rho'_1 = \frac{1}{N_1} \Pi_{\mathcal{H}'} \rho_1 \Pi_{\mathcal{H}'}, \quad \eta'_1 = \frac{N_1 \eta_1}{N}, \quad N_1 = \text{Tr}(\rho_1 \Pi_{\mathcal{H}'}) \quad (3.7)$$

$$N = N_0 \eta_0 + N_1 \eta_1. \quad (3.8)$$

And finally, the optimal failure probability Q^{opt} can be written in terms of Q'^{opt} , the optimal failure probability of the reduced problem, as

$$Q^{opt} = 1 - N + N Q'^{opt}. \quad (3.9)$$

Proof To prove the reduction theorem, we first need to recall that a USD measurement described by the POVM $\{E_k\}$ satisfies $\text{Tr}(E_0\rho_1) = 0$ and $\text{Tr}(E_1\rho_0) = 0$ by definition. It means, as a consequence of Lemma 1 given in the previous chapter, that $S_{E_0} \perp S_{\rho_1}$ and $S_{E_1} \perp S_{\rho_0}$. Since \mathcal{H}_\cap is a subspace of S_{ρ_0} and S_{ρ_1} , it follows that $S_{E_0} \perp \mathcal{H}_\cap$ and $S_{E_1} \perp \mathcal{H}_\cap$. Therefore, by writing the block-matrices in $\mathcal{H} = \mathcal{H}_\cap \oplus \mathcal{H}'$, we have

$$E_0 = \begin{pmatrix} 0 & 0 \\ 0 & E'_0 \end{pmatrix} \quad (3.10)$$

$$E_1 = \begin{pmatrix} 0 & 0 \\ 0 & E'_1 \end{pmatrix} \quad (3.11)$$

The completeness relation on \mathcal{H} implies firstly

$$E_? = \begin{pmatrix} \mathbb{1}_{\mathcal{H}_\cap} & 0 \\ 0 & E'_? \end{pmatrix} = \Pi_{\mathcal{H}_\cap} + E'_? \quad (3.12)$$

and secondly by the completeness relation on the reduced subspace \mathcal{H}'

$$\sum_k E'_k = \mathbb{1}_{\mathcal{H}'}. \quad (3.13)$$

It follows also that the operators E'_k ($k = 0, 1, ?$) are positive semi-definite operators. Therefore, by definition, $\{E'_k\}$ is a POVM on \mathcal{H}' . The fact that $E_?$ is equal to identity in the subspace \mathcal{H}_\cap is here a direct consequence of the property of an USDM on \mathcal{H} . Next we will see that $\{E'_k\}$ is a POVM of a USD in \mathcal{H}' .

We define $\Pi_{\mathcal{H}_\cap}$ and $\Pi_{\mathcal{H}'}$ as the projector onto \mathcal{H}_\cap and \mathcal{H}' respectively. Thus $\Pi_{\mathcal{H}_\cap} \oplus \Pi_{\mathcal{H}'} = \mathbb{1}_{\mathcal{H}}$. For any USDM, because of the diagonal block form of the POVM, we find for Q

$$\begin{aligned} Q &= \eta_0 \text{Tr}(\rho_0 E_?) + \eta_1 \text{Tr}(\rho_1 E_?) \\ &= (1 - N_0)\eta_0 + (1 - N_1)\eta_1 \\ &\quad + (N_0\eta_0 + N_1\eta_1)(\eta'_0 \text{Tr}(\rho'_0 E'_?) + \eta'_1 \text{Tr}(\rho'_1 E'_?)) \end{aligned} \quad (3.14)$$

$$\text{with } \rho'_0 = \frac{1}{\text{Tr}(\rho_0 \Pi_{\mathcal{H}'})} \Pi_{\mathcal{H}'} \rho_0 \Pi_{\mathcal{H}'} \quad (3.15)$$

$$\rho'_1 = \frac{1}{\text{Tr}(\rho_1 \Pi_{\mathcal{H}'})} \Pi_{\mathcal{H}'} \rho_1 \Pi_{\mathcal{H}'}. \quad (3.16)$$

Here η'_i ($i = 0, 1$) is the *a priori* probability corresponding to the new density matrix ρ'_i ($\eta'_0 + \eta'_1 = 1$)

$$\eta'_0 = \frac{N_0\eta_0}{N_0\eta_0 + N_1\eta_1}, N_0 = \text{Tr}(\rho_0 \Pi_{\mathcal{H}'}) \quad (3.17)$$

$$\eta'_1 = \frac{N_1\eta_1}{N_0\eta_0 + N_1\eta_1}, N_1 = \text{Tr}(\rho_1 \Pi_{\mathcal{H}'}). \quad (3.18)$$

We notice that $\mathcal{S}_{\rho'_0} \cap \mathcal{S}_{\rho'_1} = 0$. Moreover, $\text{Tr}(\rho_0 E_1) = 0$ implies $\text{Tr}(\rho'_0 E'_1) = 0$ and $\text{Tr}(\rho_1 E_0) = 0$ implies $\text{Tr}(\rho'_1 E'_0) = 0$. Then $\{E'_k\}$ defines a POVM describing a USDM on $\{\rho'_i, \eta'_i\}$ in \mathcal{H}' . The problem is now reduced to the subspace \mathcal{H}' . We now focus our attention on the optimality of the reduced USDM.

We can write Q as

$$\begin{aligned} Q &= (1 - N_0)\eta_0 + (1 - N_1)\eta_1 + (N_0\eta_0 + N_1\eta_1)Q' \\ &= 1 - N + NQ' \end{aligned} \quad (3.19)$$

where $Q' = \eta'_0 \text{Tr}(\rho'_0 E'_2) + \eta'_1 \text{Tr}(\rho'_1 E'_2)$ is, by definition, the failure probability of discriminating unambiguously ρ'_0 and ρ'_1 in \mathcal{H}' with *a priori* probabilities η'_0, η'_1 .

The previous equality implies that the failure probability Q is minimal if and only if the failure probability Q' is minimal. Thus we have that $\{E_k\}$ describes an optimal USDM on $\{\rho_i, \eta_i\} \Leftrightarrow Q$ is minimal $\Leftrightarrow Q'$ is minimal $\Leftrightarrow \{E'_k\}$ describes an optimal USDM on $\{\rho'_i, \eta'_i\}$. This completes the proof. ■

Let us note here that two subspaces that do not have a common subspace are not necessarily orthogonal. The formal statement is $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\} \nRightarrow \mathcal{S}_{\rho_0} \perp \mathcal{S}_{\rho_1}$. Moreover we can give an easy way to know whether the two supports overlap of ρ_0 and ρ_1 . In fact, it suffices to check whether the equation $\dim(\mathcal{H}) = \text{rank}(\rho_0) + \text{rank}(\rho_1) = \text{rank}(\rho_0 + \rho_1)$ holds. Marsaglia and Styan proved that additivity of rank of two matrices is related to the intersection of their column and row spaces in a simple way [44]. Their result is given in the following theorem.

Theorem 10 *Let A and B be two complex $m \times n$ matrices. Let \mathcal{C}_A and \mathcal{C}_B be their column spaces and \mathcal{R}_A and \mathcal{R}_B , their row spaces then*

$$\text{rank}(A + B) = \text{rank}(A) + \text{rank}(B) \text{ if and only if } \dim(\mathcal{C}_A \cap \mathcal{C}_B) = \dim(\mathcal{R}_A \cap \mathcal{R}_B) = \{0\}.$$

In the more restricted case of two density matrices, which are Hermitian matrices, the column and row spaces simply are the support $\mathcal{C}_\rho = \mathcal{R}_\rho = \mathcal{S}_\rho$.

3.2 Trivial orthogonal subspaces of the supports

We now consider the case where the supports of the two density matrices have no common subspace. That can always be achieved thanks to the previous reduction theorem for common subspace. If there is a part of \mathcal{S}_{ρ_1} orthogonal to \mathcal{S}_{ρ_0} , we can decompose \mathcal{S}_{ρ_1} into this subspace and another one (see Fig. 3.2). It turns out that this subspace of \mathcal{S}_{ρ_1} orthogonal to \mathcal{S}_{ρ_0} can be split off and leads to an unambiguous discrimination without error. The same is true for \mathcal{S}_{ρ_0} .

Theorem 11 *Reduction Theorem for Orthogonal Subspaces*

Suppose we are given two density matrices ρ_0 and ρ_1 in \mathcal{H} with a priori probabilities η_0 and η_1 . Assuming that their supports \mathcal{S}_{ρ_0} and \mathcal{S}_{ρ_1} have no common subspace, one can construct a decomposition

$$\mathcal{H} = \mathcal{H}' \oplus \mathcal{H}'^\perp \quad (3.20)$$

with $\mathcal{H}'^\perp = \mathcal{S}_0^\perp \oplus \mathcal{S}_1^\perp$, $\mathcal{S}_0^\perp = \mathcal{K}_{\rho_0} \cap \mathcal{S}_{\rho_1}$ and $\mathcal{S}_1^\perp = \mathcal{K}_{\rho_1} \cap \mathcal{S}_{\rho_0}$.

The solution of the optimal USDM problem can be given, with help of $\Pi_{\mathcal{S}_0^\perp}$ and $\Pi_{\mathcal{S}_1^\perp}$, the projection onto \mathcal{S}_0^\perp and \mathcal{S}_1^\perp , respectively, in $\mathcal{H} = \mathcal{H}' \oplus \mathcal{H}'^\perp$, by

$$E_0^{opt} = E_0'^{opt} + \Pi_{\mathcal{S}_1^\perp} \quad (3.21)$$

$$E_1^{opt} = E_1'^{opt} + \Pi_{\mathcal{S}_0^\perp} \quad (3.22)$$

$$E_?^{opt} = E_?'^{opt}. \quad (3.23)$$

The operators $E_0'^{opt}, E_1'^{opt}, E_?'^{opt}$ form a POVM $\{E_k'^{opt}\}$ with support on \mathcal{H}' describing the OptUSDM of a reduced problem defined by

$$\rho'_0 = \frac{1}{N_0} \Pi_{\mathcal{H}'} \rho_0 \Pi_{\mathcal{H}'}, \quad \eta'_0 = \frac{N_0 \eta_0}{N}, \quad N_0 = \text{Tr}(\rho_0 \Pi_{\mathcal{H}'}) \quad (3.24)$$

$$\rho'_1 = \frac{1}{N_1} \Pi_{\mathcal{H}'} \rho_1 \Pi_{\mathcal{H}'}, \quad \eta'_1 = \frac{N_1 \eta_1}{N}, \quad N_1 = \text{Tr}(\rho_1 \Pi_{\mathcal{H}'}) \quad (3.25)$$

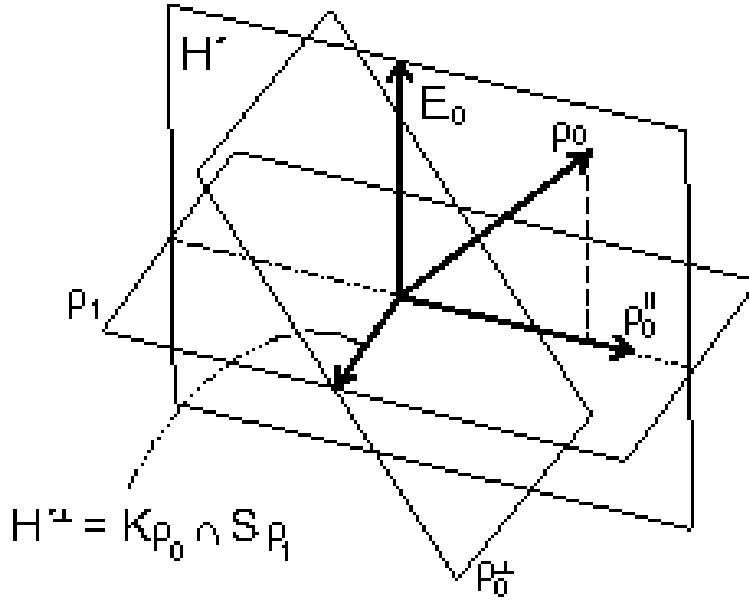
$$N = N_0 \eta_0 + N_1 \eta_1. \quad (3.26)$$

And finally, the optimal failure probability Q^{opt} can be written in terms of Q'^{opt} , the optimal failure probability of the reduced problem as

$$Q^{opt} = N Q'^{opt}. \quad (3.27)$$

Proof We translate the problem using a Naimark extension and a projection-valued measure (PVM). This idea is inspired by the first work of Sun *et al.* [32] where an extended Hilbert space has been used. Let us repeat the Naimark theorem.

Given a POVM $\{E_k\}$ on a Hilbert space \mathcal{H} , it exists an embedding of \mathcal{H} into a larger Hilbert space \mathcal{R} such that the measurement can be described by projections onto orthogonal subspaces in \mathcal{R} . More precisely, there exist a Hilbert space \mathcal{R} , an embedding \mathcal{E} such that $\mathcal{E}\mathcal{H} = \mathcal{R}$ and a PVM $\{R_k\}$ in \mathcal{R} such that with P , the projection defined by $P\mathcal{R} = \mathcal{H}$, $E_k = PR_kP, \forall k$.

Figure 3.2: Illustration of the subspace $\mathcal{K}_{\rho_0} \cap \mathcal{S}_{\rho_1}$

To the three POVM elements E_k in \mathcal{H} correspond three PVM elements R_k in \mathcal{R} . The Hilbert space \mathcal{R} can be decomposed into orthogonal subspaces

$$\mathcal{R} = \mathcal{S}_{R_0} \oplus \mathcal{S}_{R_1} \oplus \mathcal{S}_{R_2} \quad (3.28)$$

which give rise to non-orthogonal subspaces in \mathcal{H} as $\mathcal{S}_{E_k} = P\mathcal{S}_{R_k}P$. We can therefore translate properties of the USD POVM to the embedding of \mathcal{H} into \mathcal{R} .

Next we take a look at the embedding of \mathcal{S}_{ρ_0} and \mathcal{S}_{ρ_1} into \mathcal{R} and we translate the conditions for an USDM into the embedded language. We denote the embedded subspaces of \mathcal{R} by the same symbol as the original subspace of \mathcal{H} . We can here introduce the projector P^\perp onto the orthogonal complement \mathcal{H}^\perp of \mathcal{H} in \mathcal{R} ($P + P^\perp = \mathbb{1}_{\mathcal{R}}$). Since $\mathcal{S}_{\rho_0} \in \mathcal{H}$, we have $\text{Tr}(\rho_0 R_1) = \text{Tr}(P\rho_0 P R_1) = \text{Tr}(\rho_0 E_1) = 0$. This implies that \mathcal{S}_{ρ_0} is orthogonal to \mathcal{S}_{R_1} . Similarly, we find that \mathcal{S}_{ρ_1} is orthogonal to \mathcal{S}_{R_0} . Therefore, we can write

$$\mathcal{S}_{\rho_0} \subset \mathcal{S}_{R_0} \oplus \mathcal{S}_{R_{20}} \quad (3.29)$$

$$\mathcal{S}_{\rho_1} \subset \mathcal{S}_{R_1} \oplus \mathcal{S}_{R_{21}} \quad (3.30)$$

where $\mathcal{S}_{R_{20}}$ and $\mathcal{S}_{R_{21}}$ are defined as subspaces of \mathcal{S}_{R_2} with minimal dimension fulfilling the above decompositions in the sense that $\mathcal{S}_{R_{2i}} = \text{Support}(\Pi_{\mathcal{S}_{R_2}} \Pi_{\mathcal{S}_{\rho_i}} \Pi_{\mathcal{S}_{R_2}})$ for $i = 0, 1$.

The optimality condition means in particular that no information should be obtained from the conditional states following an inconclusive result. If the two failure spaces $\mathcal{S}_{R_{20}}$ and $\mathcal{S}_{R_{21}}$ are

different, it will be possible to distinguish the conditional states which arise from a projection onto $\mathcal{S}_{R_?}$ [32]. Indeed a detection in an orthogonal direction to one of the two subspaces will tell us which failure space was it or equivalently which state was sent. Therefore the optimality condition implies that $\mathcal{S}_{R_{?0}} = \mathcal{S}_{R_{?1}}$ and then

$$\mathcal{S}_{R_?} = \mathcal{S}_{R_{?0}} = \mathcal{S}_{R_{?1}}. \quad (3.31)$$

This is an important necessary condition for the optimality of a USD POVM. In the framework of the Naimark extension, this condition translates as follows. The equality of $\mathcal{S}_{R_{?0}}$ and $\mathcal{S}_{R_{?1}}$ implies that a subspace $\mathcal{S}_0^\perp = \mathcal{K}_{\rho_0} \cap \mathcal{S}_{\rho_1}$ satisfies $\mathcal{S}_0^\perp \subset \mathcal{S}_{R_1}$ in order to assure that the overlap between any state in \mathcal{S}_0^\perp and any state in \mathcal{S}_{ρ_0} will be zero. Similarly, $\mathcal{S}_1^\perp = \mathcal{K}_{\rho_1} \cap \mathcal{S}_{\rho_0} \subset \mathcal{S}_{R_0}$.

Then there exist two subspaces \mathcal{H}_1 in \mathcal{S}_{R_1} and \mathcal{H}_0 in \mathcal{S}_{R_0} such that

$$\mathcal{S}_{R_1} = \mathcal{S}_0^\perp \oplus \mathcal{H}_1 \quad (3.32)$$

$$\mathcal{S}_{R_0} = \mathcal{S}_1^\perp \oplus \mathcal{H}_0. \quad (3.33)$$

The orthogonal projection R_1 then can be decomposed into a sum of orthogonal projectors as $\Pi_{\mathcal{S}_0^\perp} + \Pi_{\mathcal{H}_1}$, with $\Pi_{\mathcal{S}_0^\perp} \Pi_{\mathcal{H}_1} = 0$, and the orthogonal projection R_0 as $\Pi_{\mathcal{S}_1^\perp} + \Pi_{\mathcal{H}_0}$, with $\Pi_{\mathcal{S}_1^\perp} \Pi_{\mathcal{H}_0} = 0$. These projectors are mapped into \mathcal{H} via the projection P . Since \mathcal{S}_i^\perp is already in \mathcal{H} , we have $P \Pi_{\mathcal{S}_i^\perp} P = \Pi_{\mathcal{S}_i^\perp}$. We define $E'_i = P \Pi_{\mathcal{H}_i} P$, $\forall i = 0, 1$ so that

$$E_0 = E'_0 + \Pi_{\mathcal{S}_1^\perp} \quad (3.34)$$

$$E_1 = E'_1 + \Pi_{\mathcal{S}_0^\perp}. \quad (3.35)$$

Furthermore, the two supports $\mathcal{S}_{E'_0}$ and \mathcal{S}_1^\perp are orthogonal since $\Pi_{\mathcal{H}_0} \Pi_{\mathcal{S}_1^\perp} = 0$ implies $\Pi_{\mathcal{H}_0} P \Pi_{\mathcal{S}_1^\perp} P = 0$ so that $P \Pi_{\mathcal{H}_0} P \Pi_{\mathcal{S}_1^\perp} P = E'_0 \Pi_{\mathcal{S}_1^\perp} = 0$. Similarly the two supports $\mathcal{S}_{E'_1}$ and \mathcal{S}_0^\perp are orthogonal too.

Moreover, $\mathcal{S}_{E_0} \perp \mathcal{S}_{\rho_1}$ and $\mathcal{S}_0^\perp \in \mathcal{S}_{\rho_1}$ so that $\mathcal{S}_{E_0} \perp \mathcal{S}_0^\perp$. Similarly, we have $\mathcal{S}_{E_1} \perp \mathcal{S}_1^\perp$. Then E'_0 and E'_1 have support on a subspace \mathcal{H}' , which is the complementary orthogonal subspace of $\mathcal{H}'^\perp = \mathcal{S}_0^\perp \oplus \mathcal{S}_1^\perp$.

Therefore in $\mathcal{H} = \mathcal{H}' \oplus \mathcal{S}_0^\perp \oplus \mathcal{S}_1^\perp = \mathcal{H}' \oplus \mathcal{H}'^\perp$, we find

$$E_0 = \begin{pmatrix} E'_0 & 0 & 0 \\ 0 & \mathbb{1}_{\mathcal{S}_1^\perp} & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (3.36)$$

$$E_1 = \begin{pmatrix} E'_1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \mathbb{1}_{\mathcal{S}_0^\perp} \end{pmatrix}. \quad (3.37)$$

From here, we will follow the same argumentation as we used in the proof of Theorem 9. The completeness relation on \mathcal{H} implies firstly

$$E_? = \begin{pmatrix} E'_? & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (3.38)$$

and secondly the completeness relation on the reduced subspace \mathcal{H}'

$$\sum_k E'_k = \mathbb{1}_{\mathcal{H}'}. \quad (3.39)$$

It follows also that the E'_k ($k = 0, 1, ?$) are positive semi-definite operators. Therefore, by definition, $\{E'_k\}$ is a POVM on \mathcal{H}' .

Let us note that $\mathcal{S}_{\rho_0} \subset \mathcal{S}_1^\perp \oplus \mathcal{H}_0 \oplus \mathcal{S}_{R_{?0}}$ and $\mathcal{S}_{\rho_1} \subset \mathcal{S}_0^\perp \oplus \mathcal{H}_1 \oplus \mathcal{S}_{R_{?1}}$. The fact that $\mathcal{S}_1^\perp \subset \mathcal{S}_{\rho_0}$ implies that

$$\mathcal{S}_{\rho_0} = \mathcal{S}_1^\perp \oplus \mathcal{H}_0', \quad (3.40)$$

with $\mathcal{H}_0' \subset \mathcal{H}_0 \oplus \mathcal{S}_{R_{?0}}$. In the same way, with $\mathcal{H}_1' \subset \mathcal{H}_1 \oplus \mathcal{S}_{R_{?1}}$,

$$\mathcal{S}_{\rho_1} = \mathcal{S}_0^\perp \oplus \mathcal{H}_1'. \quad (3.41)$$

Therefore, we can introduce a reduced problem onto \mathcal{H}' defined such that $\mathcal{H} = \mathcal{H}' \oplus \mathcal{S}_0^\perp \oplus \mathcal{S}_1^\perp$.

For any USDM, because of the diagonal block form of the POVM, we find for Q

$$\begin{aligned} Q &= \eta_0 \text{Tr}(\rho_0 E_?) + \eta_1 \text{Tr}(\rho_1 E_?) \\ &= (N_0 \eta_0 + N_1 \eta_1) (\eta'_0 \text{Tr}(\rho'_0 E'_?) + \eta'_1 \text{Tr}(\rho'_1 E'_?)) \end{aligned} \quad (3.42)$$

$$\text{with } \rho'_0 = \frac{1}{\text{Tr}(\rho_0 \Pi_{\mathcal{H}'})} \Pi_{\mathcal{H}'} \rho_0 \Pi_{\mathcal{H}'} \quad (3.43)$$

$$\rho'_1 = \frac{1}{\text{Tr}(\rho_1 \Pi_{\mathcal{H}'})} \Pi_{\mathcal{H}'} \rho_1 \Pi_{\mathcal{H}'}. \quad (3.44)$$

Here η'_i ($i = 0, 1$) is the *a priori* probability corresponding to the new density matrix ρ'_i ($\eta'_0 + \eta'_1 = 1$)

$$\eta'_0 = \frac{N_0 \eta_0}{N_0 \eta_0 + N_1 \eta_1}, N_0 = \text{Tr}(\rho_0 \Pi_{\mathcal{H}'}) \quad (3.45)$$

$$\eta'_1 = \frac{N_1 \eta_1}{N_0 \eta_0 + N_1 \eta_1}, N_1 = \text{Tr}(\rho_1 \Pi_{\mathcal{H}'}). \quad (3.46)$$

Moreover, $\text{Tr}(\rho_0 E_1) = 0$ implies $\text{Tr}(\rho'_0 E'_1) = 0$ and $\text{Tr}(\rho_1 E_0) = 0$ implies $\text{Tr}(\rho'_1 E'_0) = 0$. Then $\{E'_k\}$ defines a POVM describing a USDM on $\{\rho'_i\}$ in \mathcal{H}' .

We can rewrite the failure probability Q as

$$Q = (N_0\eta_0 + N_1\eta_1)Q' \quad (3.47)$$

where $Q' = \eta'_0 \text{Tr}(\rho'_0 E'_?) + \eta'_1 \text{Tr}(\rho'_1 E'_?)$ is, by definition, the failure probability of discriminating unambiguously ρ'_0 and ρ'_1 in \mathcal{H}' with *a priori* probabilities η'_0 and η'_1 , respectively.

And again, we have that $\{E_k\}$ describes an optimal USD on $\{\rho_i, \eta_i\} \Leftrightarrow Q$ is minimal $\Leftrightarrow Q'$ is minimal $\Leftrightarrow \{E'_k\}$ describes an optimal USD on $\{\rho'_i, \eta'_i\}$. This completes the proof. ■

3.3 Block diagonal structure

It is possible to state a last geometrical theorem which deals with two block diagonal density matrices ρ_0 and ρ_1 . Schematically, ρ_0 and ρ_1 are then of the form

$$\begin{pmatrix} \square & 0 & 0 \\ 0 & \square & 0 \\ 0 & 0 & \square \end{pmatrix}.$$

The problem of unambiguously discriminating such two density matrices can be reduced to smaller USD problems onto each one of the orthogonal subspaces. This is made more precise in the next theorem.

Theorem 12 *Reduction Theorem for two block diagonal density matrices*

Suppose we are given two density matrices ρ_0 and ρ_1 in \mathcal{H} with a priori probabilities η_0 and η_1 . Suppose that ρ_0 and ρ_1 are block diagonal (in other words, it exists a set of orthogonal projectors $\{\Pi_k\}$ such that $\sum_{k=1}^n \Pi_k = \mathbb{1}$ and $\rho_i = \sum_{k=1}^n \Pi_k \rho_i \Pi_k$, $i = 0, 1$). Then the optimal USD measurement can be chosen block diagonal where each block is optimal onto its restricted subspace.

More precisely, the optimal USD measurement is characterized by POVM elements of the form

$$E_i^{opt} = \sum_k E_i^{k, opt}. \quad (3.48)$$

For $k = 1, \dots, n$, the operators $E_0^{k, opt}, E_1^{k, opt}, E_2^{k, opt}$ form a POVM $\{E_j^{k, opt}\}$ with support on \mathcal{S}_{Π_k} describing the OptUSDM of the reduced problem defined by

$$\rho_0^k = \frac{1}{N_0^k} \Pi_k \rho_0 \Pi_k, \quad \eta_0^k = \frac{N_0^k \eta_0}{N^k}, \quad N_0^k = \text{Tr}(\rho_0 \Pi_k) \quad (3.49)$$

$$\rho_1^k = \frac{1}{N_1^k} \Pi_k \rho_1 \Pi_k, \quad \eta_1^k = \frac{N_1^k \eta_1}{N^k}, \quad N_1^k = \text{Tr}(\rho_1 \Pi_k) \quad (3.50)$$

$$N^k = N_0^k \eta_0 + N_1^k \eta_1. \quad (3.51)$$

And finally, the optimal failure probability can be written in terms of $Q^{k, opt}$, the failure probability of the reduced problems, as

$$Q^{opt} = \sum_k N_k Q_k^{opt}. \quad (3.52)$$

Proof We start with two block diagonal mixed states ρ_0 and ρ_1 with a priori probabilities η_0 and η_1 . In other words, we assume that it exists a set of orthogonal projectors $\{\Pi_k\}$ such that $\sum_{k=1}^n \Pi_k = \mathbb{1}$ and $\rho_i = \sum_{k=1}^n \Pi_k \rho_i \Pi_k$, $i = 0, 1$. Next, we denote \mathcal{S}_{Π_k} , the support of the projector Π_k . We first show that only the restriction of the POVM to the n orthogonal subspaces \mathcal{S}_{Π_k} is relevant to the failure probability. Then we will show that optimality on each orthogonal subspace \mathcal{S}_{Π_k} leads to optimality on the total Hilbert space. Let us consider a USD POVM $\{E_j\}$ onto \mathcal{H} and its failure probability Q which can be written

$$\begin{aligned}
Q &= \sum_i \eta_i \text{Tr}(E_? \rho_i) \\
&= \sum_i \eta_i \text{Tr}(E_? (\sum_k \Pi_k \rho_i \Pi_k)) \\
&= \sum_k \sum_i \eta_i \text{Tr}(\Pi_k E_? \Pi_k \rho_i \Pi_k)
\end{aligned} \tag{3.53}$$

We can obviously define n reduced density matrices onto the n subspaces \mathcal{S}_{Π_k} as

$$\rho_i^k = \frac{\Pi_k \rho_i \Pi_k}{N_i^k} \tag{3.54}$$

$$\eta_i^k = \frac{N_i^k \eta_i}{N^k} \tag{3.55}$$

$$N_i^k = \text{Tr}(\Pi_k \rho_i) \tag{3.56}$$

with $N_k = \sum_i N_i^k \eta_i$. We can also consider the restrictions of the POVM elements E_0, E_1 and $E_?$ onto those n subspaces. Thus

$$E_0^k = \Pi_k E_0 \Pi_k \tag{3.57}$$

$$E_1^k = \Pi_k E_1 \Pi_k$$

$$E_?^k = \Pi_k E_? \Pi_k.$$

Obviously those operators E_i^k ($i = 0, 1, ?$) are positive semi-definite and add up to Π_k since $\sum_i E_i = \mathbb{1}$. Each restriction onto \mathcal{S}_{Π_k} of a POVM $\{E_i\}$ then forms a POVM onto the subspace \mathcal{S}_{Π_k} . Moreover $\text{Tr}(E_i^k \rho_j^k) = \text{Tr}(\Pi_k E_i \rho_j \Pi_k) = \text{Tr}(\Pi_k E_i \rho_i \Pi_k) \delta_{ij}$ since $E_i \rho_j = E_i \rho_i \delta_{ij}$ for $i, j = 0, 1$, so that the n POVMs are n USD POVMs.

As a consequence, the failure probability for any two block diagonal density matrices can be expressed in terms of the failure probabilities $Q^k = \sum_i \eta_i^k \text{Tr}(E_i^k \rho_i^k)$ of the n reduced problems as

$$Q = \sum_k N_k Q^k. \tag{3.58}$$

We can now show that if each block is optimal then the block diagonal POVM onto \mathcal{H} is optimal too.

To prove it, let us consider an optimal USD POVM onto each one of the n orthogonal subspaces \mathcal{S}_{Π_k} . We denote $Q^{k \text{ opt}}$ the optimal failure probability onto \mathcal{S}_{Π_k} . By definition of the optimal failure probability, $Q^k \geq Q^{k \text{ opt}}$ for each subspace \mathcal{S}_{Π_k} . Since both N_k and Q^k are positive numbers, this yields

$$Q \geq \sum_k N_k Q^{k \text{ opt}}. \tag{3.59}$$

This bounds can be reached for $\{E_j\}$ being the direct sum of the n optimal USD POVMs $\{E_j^k\}$ i.e. $E_j = \sum_{k=1}^n E_j^k$, $j = 0, 1, ?$. The completes the proof. ■

3.4 A standard form of USD problem

At this point, it is useful to introduce a notation to summarize our knowledge about the USD of two density matrices. We have $\mathcal{H} = \mathcal{S}_{\rho_0} + \mathcal{S}_{\rho_1}$ then $\dim(\mathcal{H}) = \dim(\mathcal{S}_{\rho_0}) + \dim(\mathcal{S}_{\rho_1}) - \dim(\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1})$. It implies, by denoting the dimension of the Hilbert space \mathcal{H} as d , that the respective ranks r_0 and r_1 of the density matrices ρ_0 and ρ_1 satisfy

$$r_0 + r_1 \geq d. \quad (3.60)$$

For example, the case of two density matrices of the same rank $(n-1)$ in an Hilbert space of dimension n described by Rudolph *et al.* [26] can be written as “ $(n-1) + (n-1) > n$ ” while the USD between one pure state and a mixed state described by Bergou *et al.* [32, 33, 34] can be characterized as the “ $1 + n = (n+1)$ ” case. We will see in the following section that important tasks in quantum information theory can be solved elegantly thanks to those three reduction theorems.

First of all, let us discuss some immediate consequences of the three above theorems. The first reduction theorem corresponds to the elimination of the common subspace. A common subspace is present when $r_0 + r_1 > d$ holds. Its dimension is $d_{\cap} = r_0 + r_1 - d$. Therefore, after elimination of that subspace, we end up in the case $r'_0 + r'_1 = d'$ with $r'_0 = r_0 - d_{\cap}$ and similarly for r'_1 and d' . Then, we can reduce the Rudolph's case of discriminating unambiguously two density matrices of the same rank $(n-1)$ in an Hilbert space of dimension n to the “ $1 + 1 = 2$ ” case of two pure states because the common subspace is $(n-2)$ -dimensional. Rudolph *et al.* [26] already noticed it in their paper. The reduction is constructive given ρ_0 and ρ_1 .

The second reduction theorem corresponds to the elimination of the orthogonal part of one support with respect to the other, i.e., $\mathcal{K}_{\rho_0} \cap \mathcal{S}_{\rho_1}$ and $\mathcal{K}_{\rho_1} \cap \mathcal{S}_{\rho_0}$. The non-empty subspaces $\mathcal{K}_{\rho_0} \cap \mathcal{S}_{\rho_1}$ and $\mathcal{K}_{\rho_1} \cap \mathcal{S}_{\rho_0}$ can be found systematically. For example, $\mathcal{K}_{\rho_0} \cap \mathcal{S}_{\rho_1}$ can be found by projecting \mathcal{S}_{ρ_0} onto \mathcal{S}_{ρ_1} and then by taking the complementary orthogonal subspace in \mathcal{S}_{ρ_2} of that projection. As a matter of fact, this assures that we can reduce a general USD problem always to that of two density matrices of the same rank r , $r \leq \min(r_0, r_1)$, in a Hilbert space of $2r$ dimensions. Indeed, if after the first reduction, the rank of ρ'_1 is bigger than the rank of ρ'_0 , then the subspace $\mathcal{K}_{\rho'_0} \cap \mathcal{S}_{\rho'_1}$ is at least of dimension $r'_1 - r'_0$ and can be eliminated. With the help of the first two reduction theorems, we can reduce any problem of discriminating unambiguously two density matrices ρ_0 and ρ_1 , with rank r_0 and r_1 respectively, in a Hilbert space \mathcal{H} , into a problem of discriminating unambiguously two density matrices ρ'_0 and ρ'_1 with rank r ($r \leq \min(r_0, r_1)$)

in $\mathcal{H}^l \subset \mathcal{H}$, a $2r$ -dimensional Hilbert space. The reduction is constructive. The first theorem allows us to split off the common subspace and the second theorem leads to the reduce problem of discriminating unambiguously two density matrices of the same rank. The third theorem tells us that if the two density matrices have a block diagonal structure, we can reduce the problem of unambiguously discriminating them to some smaller ones, each one corresponding to a block. In fact, the three reduction theorems allow us to define a *standard form* of USD problem as follows.

Definition 5 *Standard form*

Any Unambiguous State Discrimination problem of two density matrices of rank r_0 and r_1 is reducible to that of two density matrices of the same rank $r \leq \min(r_0, r_1)$ in a $2r$ -dimensional Hilbert space without **overlapping** supports, without **trivial orthogonal** subspaces and without **block diagonal** form. Such a problem is called a **standard** Unambiguous State Discrimination problem.

The expression '**trivial orthogonal** subspaces' stands for the subspaces $\mathcal{K}_{\rho_0} \cap \mathcal{S}_{\rho_1}$ and $\mathcal{K}_{\rho_1} \cap \mathcal{S}_{\rho_0}$. It is also interesting to note that the dimension of the failure space can not be greater than the lowest rank of the involved density matrices. In the language used in the proof of the second reduction theorem, we first have $E_? = PR_?P$ so that $\dim(\mathcal{S}_{E_?}) \leq \dim(\mathcal{S}_{R_?})$. Second the dimension of $\mathcal{S}_{R_{?i}}$ can not be greater than r_i because $\mathcal{S}_{R_{?i}} = \text{support}(R_? \mathcal{S}_{\rho_i} R_?)$, for $i = 0, 1$, and $\mathcal{S}_{R_?} = \mathcal{S}_{R_{?1}} = \mathcal{S}_{R_{?0}}$. Therefore $\dim \mathcal{S}_{E_?} \leq \min_i \dim \mathcal{S}_{\rho_i}$ and we can define the maximum rank of $E_?$ as

$$r_{E_?}^{\max} = \min(r_0, r_1). \quad (3.61)$$

This result looks natural considering that we can finally reduce any problem of discriminating two density matrices with rank r_0 and r_1 , respectively, to the problem of discriminating two density matrices of the same rank r , $r \leq \min_i r_i$.

Finally, a generalization to more than two density matrices can be achieved. Considering n density matrices ρ_k ($k = 0 \dots n-1$) with *a priori* probabilities η_k , we can construct n pairs of density matrices

$$\tilde{\rho}_0 = \rho_i, \quad i \in [0, \dots, n-1] \quad (3.62)$$

and

$$\tilde{\rho}_1 = \frac{\sum_{j=0, j \neq i}^{n-1} \eta_j \rho_j}{1 - \eta_i} \quad (3.63)$$

with $\tilde{\eta}_0 = \eta_i$, $\tilde{\eta}_1 = 1 - \eta_i$, and apply the two reduction theorems to these two density matrices in the following sense (notice that $\tilde{\rho}_1$ has no physical meaning). As soon as a common subspace between any $\mathcal{S}_{\tilde{\rho}_0}$ and $\mathcal{S}_{\tilde{\rho}_1}$ exists, we can split it off from all the \mathcal{S}_{ρ_i} 's because if we cannot

discriminate unambiguously this part of the support of $\tilde{\rho}_0$ and $\tilde{\rho}_1$ then we can not discriminate unambiguously between this part of the support of all the ρ_j . The second theorem must be used more carefully. As soon as a subspace of $\mathcal{S}_{\tilde{\rho}_0}$ is orthogonal to $\mathcal{S}_{\tilde{\rho}_1}$ ($\mathcal{K}_{\tilde{\rho}_1} \cap \mathcal{S}_{\tilde{\rho}_0} \neq \{0\}$), we can eliminate it from the problem because it is orthogonal to the supports of all the ρ_j , $j \neq i$. However we cannot eliminate a subspace of $\mathcal{S}_{\tilde{\rho}_1}$ orthogonal to $\mathcal{S}_{\tilde{\rho}_0}$ ($\mathcal{K}_{\tilde{\rho}_0} \cap \mathcal{S}_{\tilde{\rho}_1} \neq \{0\}$) because we know nothing about the orthogonality of this subspace for all the states in $\tilde{\rho}_1$. In other words, we can only reduce the density matrix ρ_i corresponding to $\tilde{\rho}_0$.

In the following section we are going to apply the reduction theorems to three important tasks in quantum information theory. Those tasks are State Filtering, Unambiguous Comparison of two subspaces and Unambiguous State Comparison of two pure states. We are going to see that those three tasks are reducible to some pure state case only.

3.5 Applications of the reduction theorems

3.5.1 State Filtering

Let us consider n pure states $\{|\Psi_i\rangle\}$ with *a priori* probabilities $\{p_i\}$, $i = 0, \dots, n-1$. We may want to group them in several sets and to unambiguously discriminate among these sets. This task is called *State Filtering* [32, 34]. The simplest case deals with two sets only where the first set contains one pure state and the second set regroups the remaining $n-1$ states. This problem was studied in various papers by Bergou *et al.* [32, 33, 34] who gave the complete solution in [34]. We derive here this last result in an extremely simple way thanks to the second reduction theorem.

We have to unambiguously discriminate the two sets $\{|\Psi_0\rangle\}$ and $\{|\Psi_i\rangle\}_{i=1, \dots, n-1}$. We can consider the density matrices corresponding to these two sets as well as their *a priori* probabilities. The first density matrix obviously is $\rho_0 = |\Psi_0\rangle\langle\Psi_0|$ with *a priori* probability $\eta_0 = p_0$. The second mixed state can be written as

$$\tilde{\rho}_1 = \sum_{i=1}^{n-1} p_i |\Psi_i\rangle\langle\Psi_i|. \quad (3.64)$$

This is not a proper density matrix since it is not normalized. We then must write $\rho_1 = \frac{\sum_{i=1}^{n-1} p_i |\Psi_i\rangle\langle\Psi_i|}{\sum_{i=1}^{n-1} p_i}$. Its *a priori* probability simply is $\eta_1 = \sum_{i=1}^{n-1} p_i = 1 - p_0$. State filtering finally is equivalent to unambiguously discriminate

$$\rho_0 = |\Psi_0\rangle\langle\Psi_0| \quad (3.65)$$

with *a priori* probability $\eta_0 = p_0$ and

$$\rho_1 = \frac{\sum_{i=1}^{n-1} p_i |\Psi_i\rangle\langle\Psi_i|}{\eta_1} \quad (3.66)$$

with *a priori* probability $\eta_1 = \sum_{i=1}^{n-1} p_i$.

After writing these two density matrices, the solution to the problem is trivial.

Indeed a consequence of Theorem 11 is that we can reduce the problem of USD between a pure state and a density matrix, a “ $1 + n = (n + 1)$ ” case, to the problem of discriminating unambiguously two pure states, a “ $1 + 1 = 2$ ” case, by splitting off $\mathcal{K}_{\rho_0} \cap \mathcal{S}_{\rho_1}$ of dimension $(n - 1)$. The two reduced states are the original pure state $|\Psi_0\rangle$ and the unit vector corresponding to the projection of ρ_0 onto the support of the mixed state ρ_1 . This unnormalized vector is given by $|\widetilde{\Psi}_0''\rangle = \Pi_1 |\Psi_0\rangle$, where Π_1 is the projector onto the support of ρ_1 . The corresponding unit vector simply is $|\Psi_0''\rangle = \frac{|\widetilde{\Psi}_0''\rangle}{\| \widetilde{\Psi}_0'' \|}$.

Theorem 11 tells us that the optimal failure probability Q^{opt} for State Filtering is given by

$$Q^{opt} = N Q^{opt}(|\Psi_0\rangle, |\Psi_0''\rangle), \quad (3.67)$$

with

$$\rho'_0 = \frac{1}{N_0} \Pi_{\mathcal{H}'} \rho_0 \Pi_{\mathcal{H}'}, \quad \eta'_0 = \frac{N_0 \eta_0}{N}, \quad N_0 = \text{Tr}(\rho_0 \Pi_{\mathcal{H}'}) \quad (3.68)$$

$$\rho'_1 = \frac{1}{N_1} \Pi_{\mathcal{H}'} \rho_1 \Pi_{\mathcal{H}'}, \quad \eta'_1 = \frac{N_1 \eta_1}{N}, \quad N_1 = \text{Tr}(\rho_1 \Pi_{\mathcal{H}'}) \quad (3.69)$$

$$N = N_0 \eta_0 + N_1 \eta_1, \quad (3.70)$$

$$\mathcal{H}' = \{|\Psi_0\rangle, |\Psi_0''\rangle\}. \quad (3.71)$$

Furthermore, the optimal failure probability for two pure states $|\Psi_0\rangle$ and $|\Psi_0''\rangle$ with *a priori* probabilities η'_0 and η'_1 is given by

$$Q^{opt}(|\Psi_0\rangle, |\Psi_0''\rangle) = \eta'_1 + \eta'_0 |\langle \Psi_0 | \Psi_0'' \rangle|^2 \text{ for } \sqrt{\frac{\eta'_1}{\eta'_0}} \leq |\langle \Psi_0 | \Psi_0'' \rangle|, \quad (3.72)$$

$$Q^{opt}(|\Psi_0\rangle, |\Psi_0''\rangle) = 2\sqrt{\eta'_0 \eta'_1} |\langle \Psi_0 | \Psi_0'' \rangle| \text{ if } |\langle \Psi_0 | \Psi_0'' \rangle| \leq \sqrt{\frac{\eta'_1}{\eta'_0}} \leq \frac{1}{|\langle \Psi_0 | \Psi_0'' \rangle|}, \quad (3.73)$$

$$Q^{opt}(|\Psi_0\rangle, |\Psi_0''\rangle) = \eta'_0 + \eta'_1 |\langle \Psi_0 | \Psi_0'' \rangle|^2 \text{ if } \frac{1}{|\langle \Psi_0 | \Psi_0'' \rangle|} \leq \sqrt{\frac{\eta'_1}{\eta'_0}}. \quad (3.74)$$

therefore the optimal failure probability Q^{opt} of the non-reduced problem becomes

$$Q^{\text{opt}} = N(\eta'_1 + \eta'_0 |\langle \Psi_0 | \Psi''_0 \rangle|^2) \text{ for } \sqrt{\frac{\eta'_1}{\eta'_0}} \leq |\langle \Psi_0 | \Psi''_0 \rangle|, \quad (3.75)$$

$$Q^{\text{opt}} = N(2\sqrt{\eta'_0 \eta'_1} |\langle \Psi_0 | \Psi''_0 \rangle|) \text{ if } |\langle \Psi_0 | \Psi''_0 \rangle| \leq \sqrt{\frac{\eta'_1}{\eta'_0}} \leq \frac{1}{|\langle \Psi_0 | \Psi''_0 \rangle|}, \quad (3.76)$$

$$Q^{\text{opt}} = N(\eta'_0 + \eta'_1 |\langle \Psi_0 | \Psi''_0 \rangle|^2) \text{ if } \frac{1}{|\langle \Psi_0 | \Psi''_0 \rangle|} \leq \sqrt{\frac{\eta'_1}{\eta'_0}}. \quad (3.77)$$

If we denote $S = \sum_{j=1}^{n-1} p_j |\langle \Psi_0 | \Psi_j \rangle|^2$, we find

$$N_0 = 1 \quad (3.78)$$

$$N_1 = \frac{S}{\eta_1 \|\widetilde{\Psi''_0}\|^2} \quad (3.79)$$

$$\eta'_0 = \frac{\eta_0 N_0}{N} = \frac{p_0}{N} \quad (3.80)$$

$$\eta'_1 = \frac{\eta_1 N_1}{N} = \frac{S}{N \|\widetilde{\Psi''_0}\|^2} \quad (3.81)$$

$$|\langle \Psi_0 | \Psi''_0 \rangle| = \|\widetilde{\Psi''_0}\|. \quad (3.82)$$

We finally end up with

$$Q^{\text{opt}} = p_0 \|\widetilde{\Psi''_0}\|^2 + \frac{S}{\|\widetilde{\Psi''_0}\|^2} \text{ if } \frac{S}{\|\widetilde{\Psi''_0}\|^4} \leq p_0, \quad (3.83)$$

$$Q^{\text{opt}} = 2\sqrt{p_0} \sqrt{S} \text{ if } S \leq p_0 \leq \frac{S}{\|\widetilde{\Psi''_0}\|^4}, \quad (3.84)$$

$$Q^{\text{opt}} = p_0 + S \text{ if } p_0 \leq S. \quad (3.85)$$

3.5.2 Unambiguous Subspace Discrimination

To unambiguously discriminate two subspaces, one has to unambiguously discriminate their respective bases. We can therefore consider the two ensembles corresponding to these two bases with a flat distribution because the basis vectors all possess the same probability of appearance. In fact we consider the projectors onto those respective bases as unnormalized mixed states and try to unambiguously discriminate them. In that sense, subspace discrimination is a special case of mixed state discrimination where the two density matrices are proportional to the projectors

onto the respective subspaces.

There is a infinite amount of basis in which one can write a projector. Therefore the difficulty is to find a suitable basis of the space spanned by the two subspaces to discriminate. Such a suitable basis is given by the so-called *canonical bases* which allow us to write the two projectors in a block diagonal form, where each block is two-dimensional. This technique was used by Rudolph *et al.* for the derivation of the upper bound on the failure probability Q . Thus the unambiguous discrimination of two subspaces can be reduced to some pure state case and, because of that, be solved.

First, let us repeat that the first two reduction theorems permit us to focus our attention on the unambiguous discrimination of two subspaces S_0 and S_1 of rank r in a $2r$ -dimensional Hilbert space. Next we choose an orthogonal basis $\{|a_i\rangle\}$ of S_0 and an orthogonal basis $\{|b_j\rangle\}$ of S_1 . The unambiguous discrimination between these two subspaces then corresponds to the unambiguous discrimination of $\rho_0 = \frac{1}{r} \sum_i |a_i\rangle\langle a_i|$ and $\rho_1 = \frac{1}{r} \sum_j |b_j\rangle\langle b_j|$.

Given two subspaces S_0 and S_1 , it is always possible to find an orthonormal basis $\{|a_i\rangle\}$ of S_0 and an orthonormal basis $\{|b_j\rangle\}$ of S_1 , called *canonical* or *principal bases* such that $\langle a_i | b_j \rangle = \cos(\theta_i) \delta_{ij}$, $\cos(\theta_i) \geq 0$. In such a basis, the projectors onto S_0 and S_1 are decomposed into a direct sum of r two-dimensional subspaces. Thanks to theorem 12, the optimal solution to USD of two pure states is the only requirement for an optimal unambiguous discrimination of S_0 and S_1 .

In fact, we can assume without loss of generality that $\langle a_i | b_j \rangle = \cos(\theta_i) \delta_{ij}$, $\cos(\theta_i) \geq 0$. Indeed, we can always construct the so-called *canonical bases* $\{|a_i\rangle\}$ and $\{|b_j\rangle\}$ for two subspaces if we follow Rudolph's technique [26]. Let X_k be the $(2r) \times r$ matrix whose columns span S_k . We then write a singular value decomposition of $X_0^\dagger X_1$,

$$X_0^\dagger X_1 = U_0 S U_1^\dagger, \quad (3.86)$$

where the U_k 's are two $r \times r$ unitaries and S is positive semi-definite and diagonal with $S_{ii} = \cos(\theta_i)$, $(\theta \in [0, 2\pi])$. Let us define the vectors $|a_i\rangle$ as the i^{th} column of $X_0 U_0$ and the vectors $|b_j\rangle$, the j^{th} column of $X_1 U_1$. The set $\{|a_i\rangle\}$, respectively $\{|b_j\rangle\}$, forms an orthonormal basis of S_0 , respectively S_1 , since it is merely a rotation of a former basis. Moreover the vectors $|a_i\rangle$ and $|b_i\rangle$ satisfy $\langle a_i | b_j \rangle = \cos(\theta_i) \delta_{ij}$. The angles θ_i are called the *canonical angles* and, the vectors $|a_i\rangle$ and $|b_i\rangle$, the *canonical vectors*. $|a_i\rangle$ and $|b_i\rangle$ together span the total Hilbert space. The fundamental property $\langle a_i | b_j \rangle = \cos(\theta_i) \delta_{ij}$ allows us to write ρ_0 and ρ_1 in a block diagonal form, where each block is spanned by $\{|a_i\rangle, |b_i\rangle\}$. Indeed, in the basis $\{|a_1\rangle, |b_1\rangle, |a_2\rangle, |b_2\rangle, \dots, |a_r\rangle, |b_r\rangle\}$, the two density matrices ρ_0 and ρ_1 takes the form

$$\rho_k = \begin{pmatrix} \square & 0 & 0 \\ 0 & \square & 0 \\ 0 & 0 & \square \end{pmatrix}$$

where, each block is a two-dimension subspace spanned by $\{|a_i\rangle |b_i\rangle\}$, orthogonal to the $r-1$ other two-dimensional subspaces $\{|a_k\rangle |b_k\rangle\}$, $k = 1, \dots, i-1, i+1, \dots, n$.

Thanks to theorem 12 we can express the failure probability of unambiguously discriminating S_0 and S_1 as

$$Q^{\text{opt}} = \sum_k N^k Q^{k \text{ opt}}, \quad (3.87)$$

where the $Q^{k \text{ opt}}$ are the optimal failure probabilities for unambiguously discriminating $|a_k\rangle$ and $|b_k\rangle$ with their corresponding *a priori* probabilities η_0^k and η_1^k .

We can easily calculate all those quantities where Π_k is the projector onto the two dimensional subspace spanned by $|a_k\rangle$ and $|b_k\rangle$. Thus

$$N_i^k = \text{Tr}(\Pi_k \rho_i) = \frac{1}{r} \quad (3.88)$$

$$N^k = \sum_i \eta_i N_i^k = \sum_i \eta_i \frac{1}{r} = \frac{1}{r} \quad (3.89)$$

$$\eta_i^k = \frac{\eta_i N_i^k}{N^k} = \eta_i. \quad (3.90)$$

Moreover, for each 2x2 subspace, the optimal failure probability between the two pure states $|a_k\rangle$ and $|b_k\rangle$ with *a priori* probabilities η_0 and η_1 is given by

$$Q^{k \text{ opt}} = \eta_1 + \eta_0 |\langle a_k | b_k \rangle|^2 \text{ for } \sqrt{\frac{\eta_1}{\eta_0}} \leq |\langle a_k | b_k \rangle|, \quad (3.91)$$

$$Q^{k \text{ opt}} = 2\sqrt{\eta_0 \eta_1} |\langle a_k | b_k \rangle| \text{ for } |\langle a_k | b_k \rangle| \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{|\langle a_k | b_k \rangle|}, \quad (3.92)$$

$$Q^{k \text{ opt}} = \eta_0 + \eta_1 |\langle a_k | b_k \rangle|^2 \text{ for } \frac{1}{|\langle a_k | b_k \rangle|} \leq \sqrt{\frac{\eta_1}{\eta_0}}. \quad (3.93)$$

In fact, the total failure probability can be expressed in terms of the *canonical angles* as

$$Q^{\text{opt}} = \frac{1}{r} \sum_i Q^{i \text{ opt}} \quad (3.94)$$

with for all $i \in [1, \dots, r]$,

$$Q^{k \text{ opt}} = \eta_1 + \eta_0 \cos^2(\theta_k) \text{ for } \frac{1}{\cos(\theta_k)} \leq \sqrt{\frac{\eta_0}{\eta_1}}, \quad (3.95)$$

$$Q^{k \text{ opt}} = 2\sqrt{\eta_0 \eta_1} \cos(\theta_k) \text{ for } \cos(\theta_k) \leq \sqrt{\frac{\eta_0}{\eta_1}} \leq \frac{1}{\cos(\theta_k)}, \quad (3.96)$$

$$Q^{k \text{ opt}} = \eta_0 + \eta_1 \cos^2(\theta_k) \text{ for } \sqrt{\frac{\eta_0}{\eta_1}} \leq \cos(\theta_k). \quad (3.97)$$

There are in conclusion numerous possible expressions (in principle 3^n) of the optimal failure probability depending on the values of the canonical angles.

3.5.3 Unambiguous State Comparison

Let us consider a set of n mixed quantum states $\{\sigma_i\}$ which occur with *a priori* probabilities $\{p_i\}$. We are given m states out of that set and want to know with certainty whether all the m states are identical or not. We name this task Unambiguous State Comparison ' m out of n ', following the terminology introduced by Kleinmann *et al.* in [28].

Such an unambiguous state comparison is a special case of unambiguous state discrimination. Indeed to decide with no errors whether the m states are all identical or not, we have to unambiguously discriminate a first mixture of only identical states from a second mixture of non identical states. More precisely, we have to unambiguously discriminate the two density matrices

$$\rho_0 = \frac{1}{\eta_0} \sum_{i=1}^n (p_i \sigma_i)^{\otimes m} \quad (3.98)$$

and

$$\rho_1 = \frac{1}{\eta_1} \left(\sum_{i=1}^n p_i \sigma_i \right)^{\otimes m} - \frac{\eta_0}{\eta_1} \rho_0 \quad (3.99)$$

where $\eta_0 = \sum_{i=1}^n p_i^m$ and $\eta_1 = 1 - \eta_0$ are introduced for normalization purpose.

In the next subsections, we are going to detail the unambiguous comparison of two pure states ('two out of two') and a special case of unambiguous comparison of n pure states (' n out of n '). We will see that those cases are reducible to some pure states scenarios and then analytically solvable.

Unambiguous Comparison of two pure states

The first case we study is the simplest situation of Unambiguous State Comparison. It involves only two pure states $|\Psi_+\rangle$ and $|\Psi_-\rangle$ with *a priori* probabilities p_+ and p_- . We know it is

always possible to write two pure states in some suitable orthonormal basis $\{|0\rangle, |1\rangle\}$ as $|\Psi_{\pm}\rangle = \alpha|0\rangle \pm \beta|1\rangle$ where α and β are real and such that $\alpha^2 + \beta^2 = 1$. We can therefore denote by Θ the (real) overlap between $|\Psi_+\rangle$ and $|\Psi_-\rangle$ as $\Theta = \langle\Psi_+|\Psi_-\rangle = 2\alpha^2 - 1$. First of all, we write the two density matrices to unambiguously discriminate. Thanks to Eqn.(3.98) and Eqn.(3.99), we can explicitly express them as

$$\rho_0 = \frac{1}{\eta_0}(p_+^2|\Psi_+\Psi_+\rangle\langle\Psi_+\Psi_+| + p_-^2|\Psi_-\Psi_-\rangle\langle\Psi_-\Psi_-|), \quad (3.100)$$

$$\rho_1 = \frac{1}{2}(|\Psi_+\Psi_-\rangle\langle\Psi_+\Psi_-| + |\Psi_-\Psi_+\rangle\langle\Psi_-\Psi_+|). \quad (3.101)$$

with $\eta_0 = p_+^2 + p_-^2$ and $\eta_1 = 2p_+p_-$ so that $\eta_0 \geq \eta_1$ since $(p_+ - p_-)^2 \geq 0$. Note that $|\Psi\Phi\rangle$ stands for $|\Psi\rangle \otimes |\Phi\rangle$. We will now show that these two mixed states are block diagonal.

In chapter 2, we have seen that there is a freedom on the state ensemble of a density matrix. More precisely, a mixed state is left unchanged under a unitary mixing of its state ensemble. Next we remark that the density matrix ρ_1 is left unchanged if one swaps $|\Psi_+\Psi_-\rangle$ and $|\Psi_-\Psi_+\rangle$. Therefore, it seems natural to use a Discrete Fourier Transform to diagonalize ρ_1 . That is why, we can consider for ρ_1 the two unnormalized vectors

$$\begin{pmatrix} \widetilde{|b_+\rangle} \\ \widetilde{|b_-\rangle} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}}|\Psi_+\Psi_-\rangle \\ \frac{1}{\sqrt{2}}|\Psi_-\Psi_+\rangle \end{pmatrix} \quad (3.102)$$

that is to say

$$\widetilde{|b_{\pm}\rangle} = \frac{1}{2}(|\Psi_+\Psi_-\rangle \pm |\Psi_-\Psi_+\rangle). \quad (3.103)$$

This yields the new state ensemble $\{\frac{1}{\sqrt{2(1\pm\Theta^2)}}, |b_{\pm}\rangle\}$ where

$$|b_{\pm}\rangle = \frac{1}{\sqrt{2(1\pm\Theta^2)}}(|b_+b_-\rangle \pm |b_-b_+\rangle). \quad (3.104)$$

We finally end up with

$$\rho_1 = \frac{1}{2}((1+\Theta^2)|b_+\rangle\langle b_+| + (1-\Theta^2)|b_-\rangle\langle b_-|). \quad (3.105)$$

It is worth noticing that, since $\langle b_+|b_-\rangle = 0$, the state vectors $|b_{\pm}\rangle$ are the eigenvectors of ρ_1 with eigenvalues $b_{\pm} = \frac{1}{2}(1 \pm \Theta^2)$.

In that form, it appears obvious that ρ_0 and ρ_1 are block-diagonal. To convince ourself, we simply write the different overlaps involved here.

$$\langle \Psi_+ \Psi_+ | b_+ \rangle = \frac{2\Theta}{\sqrt{2(1+\Theta^2)}}, \quad (3.106)$$

$$\langle \Psi_- \Psi_- | b_+ \rangle = \frac{2\Theta}{\sqrt{2(1+\Theta^2)}}, \quad (3.107)$$

$$\langle \Psi_+ \Psi_+ | b_- \rangle = 0, \quad (3.108)$$

$$\langle \Psi_- \Psi_- | b_- \rangle = 0. \quad (3.109)$$

It remains to give the optimal failure probability to unambiguously discriminate ρ_0 and ρ_1 or equivalently the failure probability to unambiguously compare two pure states $|\Psi_{\pm}\rangle$.

In fact $|b_- \rangle$ is orthogonal to ρ_0 and to $|b_+ \rangle$ or in other words $|b_- \rangle \in \mathcal{S}_{\rho_1} \cap \mathcal{K}_{\rho_0}$. Thanks to Theorem 11, we know that this direction $|b_- \rangle$ can be perfectly discriminated. This direction does not contribute to the failure probability for unambiguously comparing $|\Psi_+ \rangle$ and $|\Psi_- \rangle$. We are left with the three dimensional subspace spanned by ρ_0 and $|b_+ \rangle$. Since ρ_0 is two dimensional, Theorem 11 can again be used. It tells us that we can reduce this USD problem further and only consider the problem of two pure states $|b_+ \rangle$ and $|b''_+ \rangle$ with proper *a priori* probabilities.

We introduce here the projection $|\widetilde{b''_+}\rangle$ of $|b_+ \rangle$ onto the support of ρ_0 . The corresponding unit vector is $|b''_+ \rangle = \frac{|\widetilde{b''_+}\rangle}{\|b''_+\|}$ cited above. We proceed as we did for the case of state filtering where here Π_k is the projector onto the two dimensional subspace spanned by $|b_+ \rangle$ and $|b''_+ \rangle$.

Theorem 11 tells us that the optimal failure probability Q^{opt} is given by

$$Q^{opt} = N Q^{opt}(|b_+ \rangle, |b''_+ \rangle), \quad (3.110)$$

with

$$\rho'_0 = \frac{1}{N_0} \Pi_{\mathcal{H}'} \rho_0 \Pi_{\mathcal{H}'}, \quad \eta'_0 = \frac{N_0 \eta_0}{N}, \quad N_0 = \text{Tr}(\rho_0 \Pi_{\mathcal{H}'}) \quad (3.111)$$

$$\rho'_1 = \frac{1}{N_1} \Pi_{\mathcal{H}'} \rho_1 \Pi_{\mathcal{H}'}, \quad \eta'_1 = \frac{N_1 \eta_1}{N}, \quad N_1 = \text{Tr}(\rho_1 \Pi_{\mathcal{H}'}) \quad (3.112)$$

$$N = N_0 \eta_0 + N_1 \eta_1, \quad (3.113)$$

$$\mathcal{H}' = \{|b_+ \rangle, |b''_+ \rangle\}. \quad (3.114)$$

Let us calculate the relevant quantities N_1 , N_0 and $\langle b''_+ | b_+ \rangle$. Since $|b_+ \rangle$ is an eigenvector of ρ_1 , N_1 simply is its eigenvalue. Thus

$$N_1 = \frac{1+\Theta^2}{2}. \quad (3.115)$$

To find N_0 and $\langle b''_+ | b_+ \rangle$ we first have to calculate $|\widetilde{b''_+}\rangle$ and $|b''_+\rangle$. We can express $|\widetilde{b''_+}\rangle$ in the non-orthogonal basis $\{|\Psi_+\Psi_+\rangle, |\Psi_-\Psi_-\rangle\}$ of \mathcal{S}_{ρ_0} so that

$$\begin{aligned} |\widetilde{b''_+}\rangle &= \langle \Psi_+\Psi_+ | b_+ \rangle |\Psi_+\Psi_+\rangle \\ &+ \left(\frac{\langle \Psi_-\Psi_- | b_+ \rangle - \Theta^2 \langle \Psi_+\Psi_+ | b_+ \rangle}{1 - \Theta^4} \right) (|\Psi_-\Psi_-\rangle - \Theta^2 |\Psi_+\Psi_+\rangle) \\ &= \frac{2\Theta}{(1 + \Theta^2)\sqrt{2(1 + \Theta^2)}} (|\Psi_+\Psi_+\rangle + |\Psi_-\Psi_-\rangle). \end{aligned} \quad (3.116)$$

The norm of this vector therefor is

$$\sqrt{\langle \widetilde{b''_+} | \widetilde{b''_+} \rangle} = \frac{2\Theta}{1 + \Theta^2} \quad (3.117)$$

which yields

$$|b''_+\rangle = \frac{1}{\sqrt{2(1 + \Theta^2)}} (|\Psi_+\Psi_+\rangle + |\Psi_-\Psi_-\rangle). \quad (3.118)$$

Since $N_0 = \text{Tr}(\Pi_{\mathcal{H}'} \rho_0 \Pi_{\mathcal{H}'}) = \langle b''_+ | \rho_0 | b''_+ \rangle$ we simply obtain

$$N_0 = \frac{1 + \Theta^2}{2} = N_1. \quad (3.119)$$

Finally, the last relevant quantity simply is

$$\langle b''_+ | b_+ \rangle = ||\widetilde{b''_+}|| = \frac{2\Theta}{1 + \Theta^2}. \quad (3.120)$$

Considering the three possible regimes of the optimal failure probability for two pure states, we end up with Q^{opt} , the failure probability of unambiguously comparing the two pure states $|\Psi_{\pm}\rangle$, expressed as

$$Q^{opt} = \eta_0 \frac{1 + \Theta^2}{2} + \eta_1 \frac{2\Theta^2}{1 + \Theta^2} \text{ for } \frac{1 + \Theta^2}{2\Theta^2} \leq \sqrt{\frac{\eta_1}{\eta_0}}. \quad (3.121)$$

$$Q^{opt} = 2\sqrt{\eta_0\eta_1}\Theta \text{ for } \frac{2\Theta^2}{1 + \Theta^2} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1 + \Theta^2}{2\Theta^2}, \quad (3.122)$$

$$Q^{opt} = \eta_0 \frac{2\Theta^2}{1 + \Theta^2} + \eta_1 \frac{1 + \Theta^2}{2} \text{ for } \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{2\Theta^2}{1 + \Theta^2}, \quad (3.123)$$

Let us note here, that we could derive the last expressions of Q^{opt} using the result derived for State Filtering (Eqn.(3.78) to (3.85)) with the following correspondences

$$p_0 = \eta_1 \frac{1 + \Theta^2}{2}, \quad (3.124)$$

$$p_j = p_{\pm}, \quad (3.125)$$

$$S = \eta_0 \frac{2\Theta^2}{1 + \Theta^2}, \quad (3.126)$$

$$||\widetilde{\Psi''_0}|| = ||\widetilde{b''_+}|| = \frac{2\Theta}{1 + \Theta^2}. \quad (3.127)$$

In the next application of our reduction theorems to state comparison, we will use more properties of the Discrete Fourier Transform.

Unambiguous Comparison of n pure states with a simple symmetry

We propose to study the problem of comparing n linearly independent pure states $|\Psi_i\rangle$ with equal *a priori* probabilities $p_i = \frac{1}{n}$ and equal real overlaps $\Theta = \langle \Psi_i | \Psi_j \rangle, \forall i, j = 1, \dots, n$.

Related to this comparison task, Eqn.(3.98) and (3.99) tell us that there is a USD problem that involves two density matrices ρ_0 and ρ_1 and their *a priori* probabilities expressed as

$$\rho_0 = \frac{1}{n} \sum_{i=1}^n |\Psi_i \dots \Psi_i\rangle \langle \Psi_i \dots \Psi_i| \quad (3.128)$$

$$\eta_0 = \frac{1}{n^{n-1}} \quad (3.129)$$

and

$$\rho_1 = \frac{n^{n-1}}{n^{n-1} - 1} \xi^{\otimes n} - \frac{1}{n^{n-1} - 1} \rho_0 \quad (3.130)$$

$$\eta_1 = \frac{n^{n-1} - 1}{n^{n-1}} \quad (3.131)$$

where

$$\xi = \frac{1}{n} \sum_{i=1}^n |\Psi_i\rangle \langle \Psi_i|. \quad (3.132)$$

Note that ξ is not a projector since the vectors $|\Psi_i\rangle$ are in general not orthogonal. We will now show that these two density matrices are block diagonal and that their unambiguous discrimination can be reduced to n two pure states USD problems only.

Actually we can consider the cyclic permutation C that maps $|\Psi_i\rangle$ to $|\Psi_{i+1}\rangle$ for $i = 0, n-1$ and $|\Psi_n\rangle$ to $|\Psi_0\rangle$ and the Discrete Fourier Transform. From now on, all the indexes are given

modulo n to simplify the notations. In fact, it is pretty clear that both ρ_0 and ρ_1 are invariant under the cyclic permutation $C^{\otimes n}$. We can therefore, as we have already done for the comparison of two pure states, use the Discrete Fourier Transform to change the state ensemble of ρ_0 and ρ_1 . If we do so, we will see that both ρ_0 and ρ_1 are block diagonal where each block is an eigenspace of $C^{\otimes n}$. The main reason for that is that the permutation operator C is diagonalized by the Discrete Fourier Transform. Importantly, the n vectors states of ρ_0 are n eigenvectors of $C^{\otimes n}$ with distinct eigenvalues (i.e. the n roots of unity). Therefore, the n vectors states of ρ_0 are in different eigenspaces of $C^{\otimes n}$. As a matter of fact, ρ_0 and ρ_1 are block diagonal where only one vector state of ρ_0 is in each eigenspace of $C^{\otimes n}$. Thanks to theorem 11 and 12, the USD of ρ_0 and ρ_1 is reducible to n two pure states cases.

Now that the flow of the argumentation is clear, let us first that ρ_0 and ρ_1 are invariant under $C^{\otimes n}$.

First, we examine the action of $C^{\otimes n}$ on ρ_0 .

$$C^{\otimes n} \rho_0 C^{\dagger \otimes n} = C^{\otimes n} \frac{1}{n} \sum_{i=1}^n (|\Psi_i\rangle\langle\Psi_i|)^{\otimes n} C^{\dagger \otimes n} \quad (3.133)$$

$$= \frac{1}{n} \sum_{i=1}^n C^{\otimes n} (|\Psi_i\rangle\langle\Psi_i|)^{\otimes n} C^{\dagger \otimes n} \quad (3.134)$$

$$= \frac{1}{n} \sum_{i=1}^n (C|\Psi_i\rangle\langle\Psi_i|C^\dagger)^{\otimes n} \quad (3.135)$$

$$= \frac{1}{n} \sum_{i=1}^n (|\Psi_{i+1}\rangle\langle\Psi_{i+1}|)^{\otimes n} \quad (3.136)$$

$$= \frac{1}{n} \sum_{i'=1}^n (|\Psi_{i'}\rangle\langle\Psi_{i'}|)^{\otimes n} \quad (3.137)$$

$$= \rho_0 \quad (3.138)$$

where the index $n+1$ equals 1 since the indexes are given modulo n . We can also investigate the action of C the operator $\xi = \frac{1}{n} \sum_{i=1}^n |\Psi_i\rangle\langle\Psi_i|$.

$$C\xi C^\dagger = C \left(\frac{1}{n} \sum_{i=1}^n |\Psi_i\rangle\langle\Psi_i| \right) C^\dagger \quad (3.139)$$

$$= \frac{1}{n} \sum_{i=1}^n C|\Psi_i\rangle\langle\Psi_i|C^\dagger \quad (3.140)$$

$$= \frac{1}{n} \sum_{i'=1}^n |\Psi_{i'}\rangle\langle\Psi_{i'}| \quad (3.141)$$

$$= \xi. \quad (3.142)$$

Since ξ is invariant under C , $\xi^{\otimes n}$ is invariant under $C^{\otimes n}$. $\rho_1 = \frac{n^{n-1}}{n^{n-1}-1}\xi^{\otimes n} - \frac{1}{n^{n-1}-1}\rho_0$ where both $\xi^{\otimes n}$ and ρ_0 are invariant under $C^{\otimes n}$, the immediate consequence is that ρ_1 is invariant under $C^{\otimes n}$ too.

The Discrete Fourier Transform is the main tool of the next calculations. The matrix elements of U are given by

$$U_{jk} = \frac{1}{\sqrt{n}} e^{2i\pi \frac{(j-1)(k-1)}{n}}, \quad k = 1, \dots, n. \quad (3.143)$$

The eigenvalues of C simply are the n roots of unity which can be expressed as

$$\lambda_j = e^{-2i\pi \frac{k-1}{n}}, \quad k = 1, \dots, n. \quad (3.144)$$

Let us briefly derive this result. In a tensor representation, $C_{qk} = \delta_{(q+1)k}$ therefore

$$(UCU^\dagger)_{pj} = \sum_{qk} U_{pq} C_{qk} U_{kj}^\dagger \quad (3.145)$$

$$= \sum_{qk} \frac{1}{\sqrt{n}} e^{2i\pi \frac{(p-1)(q-1)}{n}} \delta_{(q+1)k} \frac{1}{\sqrt{n}} e^{-2i\pi \frac{(k-1)(j-1)}{n}} \quad (3.146)$$

$$= \frac{1}{n} \sum_q e^{2i\pi \frac{(p-1)(q-1)}{n}} e^{-2i\pi \frac{q(j-1)}{n}} \quad (3.147)$$

$$= \frac{1}{n} \sum_q e^{2i\pi q \frac{(p-1)-(j-1)}{n}} e^{-2i\pi \frac{(p-1)}{n}} \quad (3.148)$$

$$= e^{-2i\pi \frac{(p-1)}{n}} \frac{1}{n} \sum_q e^{2i\pi q \frac{(p-j)}{n}} \quad (3.149)$$

$$= e^{-2i\pi \frac{p-1}{n}} \delta_{pj} \quad (3.150)$$

where we used the relation

$$\frac{1}{n} \sum_q e^{2i\pi q \frac{(p-j)}{n}} = \delta_{pj}. \quad (3.151)$$

The unitary freedom in the ensemble of a density matrix allows us to write any density matrix $\rho = \sum_i \mu_i |\mu_i\rangle \langle \mu_i|$ as $\sum_i v_i |v_i\rangle \langle v_i|$ where

$$\sqrt{v_i} |v_i\rangle = \sum_j U_{ij} \sqrt{\mu_j} |\mu_j\rangle. \quad (3.152)$$

We now change the set of state ensemble of both ρ_0 and ρ_1 . In the former case, we use the Discrete Fourier Transform U , a $(n \times n)$ matrix acting on n non normalized vectors $\frac{1}{\sqrt{n}} |\Psi_j \dots \Psi_j\rangle$. In the later case, we use the unitary transformation U on n non normalized vectors $\frac{1}{\sqrt{n}} |\Psi_j\rangle$ to change the state ensemble of ξ and therefore to change the state ensemble of ρ_1 too.

We begin with the state ensemble of ρ_0 and its new *a priori* probabilities v_i thanks to Eqn.(1.6).

$$v_i = \frac{1}{n} \sum_{kj} \langle \Psi_k \dots \Psi_k | U_{ik}^* U_{ij} | \Psi_j \dots \Psi_j \rangle \quad (3.153)$$

$$= \frac{1}{n} \sum_{kj} U_{ik}^* U_{ij} \langle \Psi_k \dots \Psi_k | \Psi_j \dots \Psi_j \rangle \quad (3.154)$$

$$= \frac{1}{n} \left(\sum_k U_{ik}^* \sum_{j \neq k} U_{ij} \langle \Psi_k \dots \Psi_k | \Psi_j \dots \Psi_j \rangle + \sum_k U_{ik}^* U_{ik} \langle \Psi_k \dots \Psi_k | \Psi_j \dots \Psi_j \rangle \right) \quad (3.155)$$

$$= \frac{1}{n} (\Theta^n \sum_k U_{ik}^* \sum_{j \neq k} U_{ij} + \sum_k |U_{ik}|^2). \quad (3.156)$$

At that point of the calculation, two cases must be considered. On one hand there is the case where $i = 1$ and on the other hand, $i \neq 1$. Two properties of the Discrete Fourier Transform are important here. They can be summarized as

$$\sum_{j=1}^n U_{ij} = \begin{cases} \sqrt{n} & \text{if } i = 1 \\ 0 & \text{if } i \neq 1 \end{cases}, \quad (3.157)$$

$$\sum_{j=1}^n |U_{ij}|^2 = 1 \quad \forall i. \quad (3.158)$$

The above calculation of the new *a priori* probabilities v_i for $i = 1$ then leads to

$$v_1 = \frac{1}{n} (\Theta^n \sum_k U_{1k}^* \sum_{j \neq k} U_{1j} + \sum_k |U_{1k}|^2) \quad (3.159)$$

$$= \frac{1}{n} (\Theta^n \sum_k U_{1k}^* (\sqrt{n} - U_{1k}) + 1) \quad (3.160)$$

$$= \frac{1}{n} (\Theta^n (\sqrt{n} \sum_k U_{1k}^* - \sum_k |U_{1k}|^2) + 1) \quad (3.161)$$

$$= \frac{1}{n} (\Theta^n (n - 1) + 1). \quad (3.162)$$

A similar calculation for $i \neq 1$ gives

$$v_i = \frac{1}{n} (\Theta^n \sum_k U_{ik}^* \sum_{j \neq k} U_{ij} + \sum_k |U_{ik}|^2) \quad (3.163)$$

$$= \frac{1}{n} (\Theta^n \sum_k U_{ik}^* (0 - U_{ik}) + 1) \quad (3.164)$$

$$= \frac{1}{n} (-\Theta^n \sum_k |U_{ik}|^2 + 1) \quad (3.165)$$

$$= \frac{1}{n} (-\Theta^n + 1). \quad (3.166)$$

Finally, ρ_0 takes the form

$$\rho_0 = \frac{1 + (n-1)\Theta^n}{n} |\Phi_1\rangle\langle\Phi_1| + \frac{1 - \Theta^n}{n} \sum_k |\Phi_k\rangle\langle\Phi_k| \quad (3.167)$$

$$(3.168)$$

with

$$|\Phi_1\rangle = \frac{1}{\sqrt{1 + (n-1)\Theta^n}} \sum_j |\Psi_j \dots \Psi_j\rangle, \quad (3.169)$$

$$|\Phi_k\rangle = \frac{1}{\sqrt{1 - \Theta^n}} \sum_j e^{2i\pi \frac{(k-1)(j-1)}{n}} |\Psi_j \dots \Psi_j\rangle \text{ for } i \neq 1. \quad (3.170)$$

The fundamental property of those states vector $|\Phi_j\rangle$, $i = 1, \dots, n$ is that they are eigenvectors of $C^{\otimes n}$ with n distinct eigenvalues. Note here that $C^{\otimes n}$ has the same eigenvalues than C because this eigenvalues are roots of unity. In other words,

$$C^{\otimes n} |\Phi_j\rangle = \lambda_j |\Phi_j\rangle, \quad (3.171)$$

with $\lambda_j = e^{-2i\pi \frac{k-1}{n}}$, $k = 1, \dots, n$. Indeed the operator $C^{\otimes n}$ acts on the vector $|\Phi_k\rangle$ as

$$C^{\otimes n} |\Phi_k\rangle = C^{\otimes n} \frac{1}{\sqrt{1 - \Theta^n}} \sum_j e^{2i\pi \frac{(k-1)(j-1)}{n}} |\Psi_j \dots \Psi_j\rangle \quad (3.172)$$

$$= \frac{1}{\sqrt{1 - \Theta^n}} \sum_j e^{2i\pi \frac{(k-1)(j-1)}{n}} C^{\otimes n} |\Psi_j \dots \Psi_j\rangle \quad (3.173)$$

$$= \frac{1}{\sqrt{1 - \Theta^n}} \sum_j e^{2i\pi \frac{(k-1)(j-1)}{n}} C |\Psi_j\rangle \otimes \dots \otimes C |\Psi_j\rangle \quad (3.174)$$

$$= \frac{1}{\sqrt{1 + (n-1)\Theta^n}} \sum_j e^{2i\pi \frac{(k-1)(j-1)}{n}} |\Psi_{j+1} \dots \Psi_{j+1}\rangle \quad (3.175)$$

$$= \frac{1}{\sqrt{1 + (n-1)\Theta^n}} \sum_j e^{2i\pi \frac{(k-1)(j+1-1)}{n}} e^{-2i\pi \frac{k-1}{n}} |\Psi_{j+1} \dots \Psi_{j+1}\rangle \quad (3.176)$$

$$= e^{-2i\pi \frac{k-1}{n}} \frac{1}{\sqrt{1 + (n-1)\Theta^n}} \sum_{j'} e^{2i\pi \frac{(k-1)(j'-1)}{n}} |\Psi_{j'} \dots \Psi_{j'}\rangle \quad (3.177)$$

$$= e^{-2i\pi \frac{k-1}{n}} |\Phi_k\rangle \quad (3.178)$$

$$= \lambda_k |\Phi_k\rangle. \quad (3.179)$$

By definition, ρ_0 can be written in a block diagonal form where each block is an eigenspace of $C^{\otimes n}$.

We follow the same technique to change the state ensemble of ρ_1 . Since $\rho_1 = \frac{n^{n-1}}{n^{n-1}-1} \xi^{\otimes n} - \frac{1}{n^{n-1}-1} \rho_0$, we focus our interest on the matrix ξ . We use the Discrete Fourier Transform U acting

on the n unnormalized vectors $\frac{1}{\sqrt{n}}|\Psi_j\rangle$ to change the state ensemble of ξ and, as a consequence, of ρ_1 .

We calculate the new *a priori* probabilities v_i of the new state ensemble of ξ .

$$v_i = \frac{1}{n} \sum_{kj} \langle \Psi_k | U_{ik}^* U_{ij} | \Psi_j \rangle \quad (3.180)$$

$$= \frac{1}{n} \sum_{kj} U_{ik}^* U_{ij} \langle \Psi_k | \Psi_j \rangle \quad (3.181)$$

$$= \frac{1}{n} \left(\sum_k U_{ik}^* \sum_{j \neq k} U_{ij} \langle \Psi_k | \Psi_j \rangle + \sum_k U_{ik}^* U_{ik} \langle \Psi_k \dots \Psi_k | \Psi_j \dots \Psi_j \rangle \right) \quad (3.182)$$

$$= \frac{1}{n} (\Theta \sum_k U_{ik}^* \sum_{j \neq k} U_{ij} + \sum_k |U_{ik}|^2). \quad (3.183)$$

This calculation is similar to ρ_0 's case. Only the quantity Θ^n is changed to Θ . Therefore, we end up with

$$v_i = \begin{cases} \frac{1}{n}(1 + (n-1)\Theta), & i = 1 \\ \frac{1}{n}(1 - \Theta), & \forall i \neq 1. \end{cases} \quad (3.184)$$

Finally, ξ takes the form

$$\xi = \frac{1 + (n-1)\Theta}{n} |Y_1\rangle \langle Y_1| + \frac{1 - \Theta}{n} \sum_k |Y_k\rangle \langle Y_k| \quad (3.185)$$

with

$$|Y_1\rangle = \frac{1}{\sqrt{1 + (n-1)\Theta}} \sum_j |\Psi_j\rangle, \quad (3.186)$$

$$|Y_k\rangle = \frac{1}{\sqrt{1 - \Theta}} \sum_j e^{2i\pi \frac{(k-1)(j-1)}{n}} |\Psi_j\rangle \text{ for } i \neq 1. \quad (3.187)$$

The immediate consequence is that

$$\rho_1 = \frac{n^{n-1}}{n^{n-1} - 1} \left(\frac{1 + (n-1)\Theta}{n} |Y_1\rangle \langle Y_1| + \frac{1 - \Theta}{n} \sum_k |Y_k\rangle \langle Y_k| \right)^{\otimes n} \quad (3.188)$$

$$= \frac{1}{n^{n-1} - 1} \frac{1 + (n-1)\Theta^n}{n} |\Phi_1\rangle \langle \Phi_1| + \frac{1 - \Theta^n}{n} \sum_k |\Phi_k\rangle \langle \Phi_k| \quad (3.189)$$

Moreover, the state vectors $|\Psi_j\rangle$ of ξ are eigenvectors of C therefore the state vectors $|\Psi_{i1} \dots \Psi_{in}\rangle$ of $\xi^{\otimes n}$ are eigenvectors of $C^{\otimes n}$. A short calculation can verify this claim.

$$C|\Phi_j\rangle = C \sum_j U_{jk} |\Psi_k\rangle \quad (3.190)$$

$$= \sum_k U_{jk} C |\Psi_k\rangle \quad (3.191)$$

$$= \sum_k U_{jk} |\Psi_{k+1}\rangle \quad (3.192)$$

$$= \sum_k e^{2i\pi \frac{(j-1)(k-1)}{n}} |\Psi_{k+1}\rangle \quad (3.193)$$

$$= \sum_k e^{2i\pi \frac{(j+1-1)(k-1)}{n}} e^{-2i\pi \frac{(k-1)}{n}} |\Psi_{k+1}\rangle \quad (3.194)$$

$$= e^{-2i\pi \frac{(j-1)}{n}} \sum_k e^{2i\pi \frac{(j-1)(k+1-1)}{n}} |\Psi_{k+1}\rangle \quad (3.195)$$

$$= e^{-2i\pi \frac{(j-1)}{n}} \sum_{k'} e^{2i\pi \frac{(j+1-1)(k'-1)}{n}} |\Psi_{k'}\rangle \quad (3.196)$$

$$= e^{-2i\pi \frac{(j-1)}{n}} |\Phi_j\rangle \quad (3.197)$$

$$= \lambda_j |\Phi_j\rangle. \quad (3.198)$$

This implies that

$$C \otimes \dots \otimes C |\Phi_{i1} \dots \Phi_{in}\rangle = C |\Phi_{i1}\rangle \otimes \dots \otimes C |\Phi_{in}\rangle \quad (3.199)$$

$$= \lambda_{i1} |\Phi_{i1}\rangle \otimes \dots \otimes \lambda_{in} |\Phi_{in}\rangle \quad (3.200)$$

$$= \lambda_{i1} \dots \lambda_{in} |\Phi_{i1} \dots \Phi_{in}\rangle \quad (3.201)$$

Since the state vectors of $\xi^{\otimes n}$ are eigenvectors of $C^{\otimes n}$, $\xi^{\otimes n}$, like ρ_0 , is block diagonal, where each block in an eigenspace of $C^{\otimes n}$. The immediate consequence is that ρ_1 , linear combination of $\xi^{\otimes n}$ and ρ_0 is block diagonal, too.

Let us denote S_k , the eigenspace associated with the eigenvalues λ_k of $C^{\otimes n}$ and Π_k the orthogonal projector onto S_k . We have

$$\rho_0 = \sum_k \Pi_k \rho_0 \Pi_k, \quad (3.202)$$

$$\rho_1 = \sum_k \Pi_k \rho_1 \Pi_k. \quad (3.203)$$

$$(3.204)$$

Therefore, Theorem 12 tells us to focus our attention onto the n reduced problem defined by the two density matrices $\rho_0^k = \frac{\Pi_k \rho_0 \Pi_k}{\text{Tr}(\Pi_k \rho_0)}$ and $\rho_1^k = \frac{\Pi_k \rho_1 \Pi_k}{\text{Tr}(\Pi_k \rho_1)}$. Moreover the reduced density matrix ρ_0^k

simply is a pure state

$$\Pi_k \rho_0 \Pi_k = |\phi_k\rangle\langle\phi_k| \quad (3.205)$$

since the n state vectors of ρ_0 are eigenvectors of $C^{\otimes n}$ with distinct eigenvalues. By means of Theorem 11, we can reduce the USD problem of unambiguously discriminating ρ_0^k and ρ_1^k to the one of two pure states only.

Finally the unambiguous discrimination of ρ_0 and ρ_1 or, equivalently, the unambiguous comparison of n linearly independent pure states $|\Psi_i\rangle$ with equal *a priori* probabilities $p_i = \frac{1}{n}$ and equal real overlaps $\Theta = \langle\Psi_i|\Psi_j\rangle, \forall i, j = 1, \dots, n$ is reducible to n two pure states cases.

The goal of this section was to show that the unambiguous comparison of n pure states with equal *a priori* probabilities and equal and real overlaps is reducible to some pure state case. As we have already indicated in the introduction, the question to know whether any unambiguous comparison of pure states is always reducible to some pure state cases remains opened. However, as expected, the unambiguous comparison of mixed states is generally not reducible to some pure states case [28].

This concludes this chapter. In the next chapter, we will derive the first class of exact solutions for a generic USD problem.

Chapter 4

First class of exact solutions

The structure of this chapter is the following. In the section 4.1, we derive three lower bounds on the failure probability to unambiguously discriminate two density matrices in three regimes of the ratio between the two *a priori* probabilities. Our derivation uses the Cauchy-Schwarz inequality and allows us to look for necessary and sufficient conditions to reach the lower bound in each regime of the *a priori* probabilities. In section 4.2, we report the notion of *parallel addition* that leads to some useful relations for USD in connection with our first reduction theorem. In section 4.3, we finally derive the main result of this chapter as a theorem: a necessary and sufficient set of two conditions for the failure probability to reach the bounds are given. We also give the corresponding optimal POVM.

With that result, we give the optimal USD POVM of a wide class of pairs of mixed states. This class corresponds to pairs of mixed states for which the lower bounds (one for each of the three regimes depending on the ratio between the *a priori* probabilities) on the failure probability Q are saturated. This class is nonempty since it contains some pairs of generic mixed states as well as any pair of pure states. For those pairs, we provide the first analytical solutions for unambiguous discrimination of generic mixed states. This goes beyond known results which are all reducible to some pure state case as we have seen in chapter 2 and 3.

4.1 Lower bounds on the failure probability

The failure probability Q of a USD strategy is given by $Q = \sum_i Q_i$, where $Q_i = \eta_i \text{Tr}(E_i \rho_i)$. From this definition we immediately see that $Q_i \leq \eta_i$. In this chapter, we consider the USD of two signal states ρ_0 and ρ_1 that are mixed states with *a priori* probabilities η_0 and η_1 . Accordingly, our POVM contains three elements $\{E_0, E_1, E_?\}$ which correspond respectively to the conclusive detection of ρ_0 , to the conclusive detection of ρ_1 and to an inconclusive result. The failure probability then equals $Q = Q_0 + Q_1$.

Our interest is first focused on the product Q_0Q_1 . We can give a lower bound expressed in terms of the fidelity $F = \text{Tr}(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}})$ of the two states ρ_0 and ρ_1 . The bounds, formulated in the following theorem, are tighter than those given in chapter 2. Moreover, we pay additional attention to the condition under which the bounds can be reached.

Theorem 13 *Lower bound on the product Q_0Q_1*

Let ρ_0 and ρ_1 be two density matrices with a priori probabilities η_0 and η_1 . We define the fidelity of the two states ρ_0 and ρ_1 as $F = \text{Tr}(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}})$. Then, for any USD measurement with inconclusive outcome $E_?$, the product of the two probabilities Q_0 and Q_1 to fail to identify respectively the state ρ_0 and ρ_1 is such that

$$Q_0Q_1 \geq \eta_0\eta_1F^2. \quad (4.1)$$

The equality holds if and only if the unitary operator V arising from a polar decomposition

$$\sqrt{\rho_0}\sqrt{\rho_1} = \sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}} V \quad (4.2)$$

satisfies

$$V^\dagger \sqrt{\rho_0} \sqrt{E_?} = \alpha \sqrt{\rho_1} \sqrt{E_?} \quad (4.3)$$

for some $\alpha \in \mathbb{R}^+$.

Before we turn to the proof of this theorem, note that relation (4.3) implies a condition on the optimality of a USD POVM [32, 33, 45]. It is clear that optimality of a specific USD measurement implies that the conditional states after the inconclusive results do not allow further USD measurements as we already discussed it in chapter 3. This condition is satisfied, for example, when the supports of the conditional states coincide. We find a stronger property whenever equality holds in Theorem 13. Indeed, if we have $V^\dagger \sqrt{\rho_0} \sqrt{E_?} = \alpha \sqrt{\rho_1} \sqrt{E_?}$ with $\alpha \in \mathbb{R}^+$, then it follows immediately that $\sqrt{E_?}\rho_0\sqrt{E_?} = \alpha^2\sqrt{E_?}\rho_1\sqrt{E_?}$. This means that the conditional states corresponding to inconclusive results must be identical up to normalization. Therefore no information whatsoever about the signal state can be extracted from these conditional states.

Proof of Theorem 13 This theorem was stimulated by the proof of the *nonbroadcasting* theorem [46]. The basic ingredient for the derivation of the bound is the Cauchy-Schwarz inequality:

Theorem 14 [47] *Cauchy-Schwarz inequality*

If x and y are members of a unitary space then $\|x\|\|y\| \geq |(x,y)|$.

The equality holds if and only if $x = \alpha y$ for some α in \mathbb{C} .

A unitary space is a complex linear space \mathcal{S} together with an inner product from $\mathcal{S} \times \mathcal{S}$ to \mathbb{C} . Therefore the complex space of bounded operators acting on a Hilbert space is a complete unitary

space (i.e. every Cauchy sequence converge) if we consider for two elements A and B the inner product $\text{Tr}(AB^\dagger)$. The Cauchy-Schwarz inequality then takes the form $\sqrt{\text{Tr}(AA^\dagger)}\sqrt{\text{Tr}(BB^\dagger)} \geq |\text{Tr}(AB^\dagger)|$ where equality holds for $A = \alpha B$, α in \mathbb{C} .

Let us now consider a POVM element E_k and two density matrices ρ_0 and ρ_1 . We can decompose these three operators as $\rho_1 = \sqrt{\rho_1}\sqrt{\rho_1}$ and $E_k = \sqrt{E_k}\sqrt{E_k}$ and $\rho_0 = \sqrt{\rho_0}UU^\dagger\sqrt{\rho_0}$ where U is an arbitrary unitary transformation coming from the freedom in the decomposition of a positive semi-definite operator. Hence we obtain from the Cauchy-Schwarz inequality with $A = U^\dagger\sqrt{\rho_0}\sqrt{E_k}$ and $B = \sqrt{\rho_1}\sqrt{E_k}$

$$\sqrt{\text{Tr}(E_k\rho_0)}\sqrt{\text{Tr}(E_k\rho_1)} \geq |\text{Tr}(U^\dagger\sqrt{\rho_0}\sqrt{E_k}\sqrt{E_k}\sqrt{\rho_1})| = |\text{Tr}(U^\dagger\sqrt{\rho_0}E_k\sqrt{\rho_1})|. \quad (4.4)$$

By Theorem 14, the equality holds if and only if $U^\dagger\sqrt{\rho_0}\sqrt{E_k} = \alpha\sqrt{\rho_1}\sqrt{E_k}$, for some $\alpha \in \mathbb{C}$.

We now consider a USD POVM $\{E_k\}_{k=0,1,?}$. Using the fact that $\text{Tr}(E_0\rho_1) = \text{Tr}(E_1\rho_0) = 0$, we find for E_0 and E_1

$$0 = \sqrt{\text{Tr}(E_0\rho_0)}\sqrt{\text{Tr}(E_0\rho_1)} \geq |\text{Tr}(U^\dagger\sqrt{\rho_0}E_0\sqrt{\rho_1})|, \quad (4.5)$$

$$0 = \sqrt{\text{Tr}(E_1\rho_0)}\sqrt{\text{Tr}(E_1\rho_1)} \geq |\text{Tr}(U^\dagger\sqrt{\rho_0}E_1\sqrt{\rho_1})|. \quad (4.6)$$

This simply means that $\text{Tr}(U^\dagger\sqrt{\rho_0}E_0\sqrt{\rho_1}) = \text{Tr}(U^\dagger\sqrt{\rho_0}E_1\sqrt{\rho_1}) = 0$. For $E_?$, we obtain

$$\sqrt{\text{Tr}(E_?\rho_0)}\sqrt{\text{Tr}(E_?\rho_1)} \geq |\text{Tr}(U^\dagger\sqrt{\rho_0}E_?\sqrt{\rho_1})|. \quad (4.7)$$

From this it follows that we can write

$$\sqrt{\text{Tr}(E_?\rho_0)}\sqrt{\text{Tr}(E_?\rho_1)} \geq |\text{Tr}(U^\dagger\sqrt{\rho_0}E_?\sqrt{\rho_1}) + 0 + 0| = |\text{Tr}(U^\dagger\sqrt{\rho_0}\sqrt{\rho_1})|, \quad (4.8)$$

where we used the relation $\sum_k E_k = \mathbb{1}$. Furthermore, the inequality (4.8) must hold for any unitary matrix U so that we find

$$\sqrt{\text{Tr}(E_?\rho_0)}\sqrt{\text{Tr}(E_?\rho_1)} \geq \max_U |\text{Tr}(U^\dagger\sqrt{\rho_0}\sqrt{\rho_1})|. \quad (4.9)$$

Here, again, the equality holds if and only if a unitary operator U_{\max} which maximizes the right hand side satisfies

$$U_{\max}^\dagger\sqrt{\rho_0}\sqrt{E_?} = \alpha\sqrt{\rho_1}\sqrt{E_?} \quad (4.10)$$

for some $\alpha \in \mathbb{C}$. To find the unitary matrices U_{\max} that maximize $|\text{Tr}(U^\dagger\sqrt{\rho_0}\sqrt{\rho_1})|$ we use the following lemma:

Lemma 2 For any operator A in the space M_n of $n \times n$ matrices we find

$$\max_W |\text{Tr}(AW)| = \text{Tr}(|A|) \quad (4.11)$$

where the maximum is taken over all unitary matrices. The maximum is reached for any unitary operator W that can be written as $W = V^\dagger e^{i\phi}$. Here $e^{i\phi}$ is an arbitrary phase while the unitary operator V is defined via a polar decomposition

$$A = |A|V \quad (4.12)$$

with $|A| = \sqrt{AA^\dagger} = V \sqrt{A^\dagger A} V^\dagger$. (See proof in Appendix B.)

Let us introduce the operators $F_0 := |\sqrt{\rho_0}\sqrt{\rho_1}| = \sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $F_1 = V^\dagger F_0 V = \sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$, which are motivated by the polar decomposition

$$\sqrt{\rho_0}\sqrt{\rho_1} = F_0 V = V F_1. \quad (4.13)$$

These operators are related to the fidelity of the two density matrices through the relation $F = \text{Tr}(\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}) = \text{Tr}(F_0) = \text{Tr}(F_1)$ [40]. Thanks to lemma 2, Eqn. (4.9) implies

$$\sqrt{\text{Tr}(E_? \rho_0)} \sqrt{\text{Tr}(E_? \rho_1)} \geq |\text{Tr}(|\sqrt{\rho_0}\sqrt{\rho_1}|)| = \text{Tr}(|\sqrt{\rho_0}\sqrt{\rho_1}|) \quad (4.14)$$

where equality now holds if and only if U_{max} in (4.10) arises from a polar decomposition of $\sqrt{\rho_0}\sqrt{\rho_1}$. In other words, we have

$$V^\dagger e^{i\phi} \sqrt{\rho_0} \sqrt{E_?} = \alpha \sqrt{\rho_1} \sqrt{E_?} \quad (4.15)$$

for some $\alpha \in \mathbb{C}$.

Next we use the definitions of the partial failure probabilities $Q_i = \eta_i \text{Tr}(E_? \rho_i)$ and choose the phase $e^{i\phi}$ to be the same as the phase of α in (4.15) to obtain the desired inequality $Q_0 Q_1 \geq \eta_0 \eta_1 F^2$. Equality in the previous equation then holds if and only if $V^\dagger \sqrt{\rho_0} \sqrt{E_?} = \alpha \sqrt{\rho_1} \sqrt{E_?}$, for some $\alpha \in \mathbb{R}^+$. This completes the proof. ■

We can now derive the bounds in the different regimes of the ratio $\frac{\eta_1}{\eta_0}$ between the two *a priori* probabilities. Actually, the procedure is to find the minimum of the failure probability $Q = Q_0 + Q_1$ under the constraints of the previous derived inequality $Q_0 Q_1 \geq \eta_0 \eta_1 F^2$. According to Theorem 13, we can provide the necessary and sufficient condition for equality.

Theorem 15 *Lower bounds on the failure probability*

Let ρ_0 and ρ_1 be two density matrices with a priori probabilities η_0 and η_1 . We define the fidelity F of the two states ρ_0 and ρ_1 as $\text{Tr}(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}})$. We denote by P_0 and P_1 , the projectors onto the support of ρ_0 and ρ_1 . Then, for any USD measurement with inconclusive outcome $E_?$, the failure probability Q obeys

$$Q \geq \eta_1 \frac{F^2}{\text{Tr}(P_1\rho_0)} + \eta_0 \text{Tr}(P_1\rho_0) \quad \text{for} \quad \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{\text{Tr}(P_1\rho_0)}{F} \quad (4.16)$$

$$Q \geq 2\sqrt{\eta_0\eta_1}F \quad \text{for} \quad \frac{\text{Tr}(P_1\rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{F}{\text{Tr}(P_0\rho_1)} \quad (4.17)$$

$$Q \geq \eta_0 \frac{F^2}{\text{Tr}(P_0\rho_1)} + \eta_1 \text{Tr}(P_0\rho_1) \quad \text{for} \quad \frac{F}{\text{Tr}(P_0\rho_1)} \leq \sqrt{\frac{\eta_1}{\eta_0}}. \quad (4.18)$$

Equality holds if and only if the unitary operator V arising from a polar decomposition $\sqrt{\rho_0}\sqrt{\rho_1} = \sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}V$ satisfies $V^\dagger\sqrt{\rho_0}\sqrt{E_?} = \alpha\sqrt{\rho_1}\sqrt{E_?}$, with $\alpha = \frac{\text{Tr}(P_1\rho_0)}{F}$, $\alpha = \sqrt{\frac{\eta_1}{\eta_0}}$ and $\alpha = \frac{F}{\text{Tr}(P_0\rho_1)}$ in the first, second and third regime, respectively.

Proof First of all, according to Theorem 13, we know that for any USD measurement the inequality $Q_0Q_1 \geq \eta_0\eta_1F^2$ i.e. $Q_1 \geq \frac{\eta_0\eta_1F^2}{Q_0}$ holds. It follows that the failure probability is lower bounded as

$$Q \geq Q_0 + \frac{\eta_0\eta_1F^2}{Q_0}. \quad (4.19)$$

Since we are interested in a lower bound on Q , let us consider the case where equality holds in Eqn. (4.19). In this case, we have

$$Q_0Q_1 = \eta_0\eta_1F^2 \quad (4.20)$$

$$Q = Q_0 + \frac{\eta_0\eta_1F^2}{Q_0} \quad (4.21)$$

From Theorem 13 we know that Eqn.(4.20) holds if and only if $V^\dagger\sqrt{\rho_0}\sqrt{E_?} = \alpha\sqrt{\rho_1}\sqrt{E_?}$, for some $\alpha \in \mathbb{R}^+$. We will now connect α to the other quantities. The previous relation implies, via the respective definitions, that

$$Q_0 = \alpha^2 \frac{\eta_0}{\eta_1} Q_1. \quad (4.22)$$

The former relationship corresponds to the proportionality between two vectors of the vector space of bounded operators while the latter relationship corresponds to the proportionality between their norms. We can combine the two equations (4.20) and (4.22) to

$$Q_0 = \alpha\eta_0F \quad (4.23)$$

$$Q_1 = \frac{1}{\alpha}\eta_1F. \quad (4.24)$$

So the final statement is that $Q = Q_0 + \frac{\eta_0 \eta_1 F^2}{Q_0}$ if and only if $V^\dagger \sqrt{\rho_0} \sqrt{E_?} = \alpha \sqrt{\rho_1} \sqrt{E_?}$, where α now is explicitly related to the other parameters as $Q_0 = \alpha \eta_0 F$ and $Q_1 = \frac{1}{\alpha} \eta_1 F$.

Second, we have to derive a range constraint on Q_0 and Q_1 . We know already that $Q_i \leq \eta_i$. Moreover, from work by Herzog and Bergou in [29], we learn that $\eta_0 \text{Tr}(P_1 \rho_0) \leq Q_0$ and $\eta_1 \text{Tr}(P_0 \rho_1) \leq Q_1$. Indeed, from the structure of the USD POVM elements, we have $E_0 + E_1 + E_? = \mathbb{1}$ with $\mathcal{S}_{E_0} \subset \mathcal{K}_{\rho_1}$ and $\mathcal{S}_{E_1} \subset \mathcal{K}_{\rho_0}$. We consider only the non-trivial case where the supports of ρ_0 and ρ_1 are not identical. Then the structure must be such that $E_1 + E_? = P_1 + R$ where P_1 is the projection onto the support of ρ_1 and R is a positive semi-definite operator with support $\mathcal{S}_R \subset \mathcal{K}_{\rho_1}$ which satisfies $E_0 + R = P_1^\perp$ otherwise $\text{Tr}(E_0 \rho_1) \neq 0$. Then it follows that the partial success probability P_0^s is $P_0^s = \eta_0 \text{Tr}(E_0 \rho_0) = \eta_0 \text{Tr}(P_1^\perp \rho_0) - \eta_0 \text{Tr}(R \rho_0)$. In our non-trivial case we will have $\text{Tr}(R \rho_0) > 0$ as soon as $R \neq 0$. This yields $P_0^s \leq \eta_0 \text{Tr}(P_1^\perp \rho_0)$ or equivalently $Q_0 \geq \eta_0 \text{Tr}(P_1 \rho_0)$. In the same way, one can find $Q_1 \geq \eta_1 \text{Tr}(P_0 \rho_1)$. We then have

$$\eta_0 \text{Tr}(P_1 \rho_0) \leq Q_0 \leq \eta_0, \quad (4.25)$$

$$\eta_1 \text{Tr}(P_0 \rho_1) \leq Q_1 \leq \eta_1. \quad (4.26)$$

These two constraints can be combined in

$$\eta_0 \text{Tr}(P_1 \rho_0) \leq Q_0 \leq \eta_0 \frac{F^2}{\text{Tr}(P_0 \rho_1)}. \quad (4.27)$$

This can be seen as follows. Since $Q_1 = \frac{\eta_0 \eta_1 F^2}{Q_0}$, the constraint (4.26) on Q_1 takes the form

$$\eta_0 F^2 \leq Q_0 \leq \eta_0 \frac{F^2}{\text{Tr}(P_0 \rho_1)}. \quad (4.28)$$

We now have two lower bounds and two upper bounds on Q_0 ((4.25) and (4.28)) and we want to find the tighter ones. To do that, let us consider the USD POVM given by $\{E_? = P_1, E_0 = P_1^\perp, E_1 = 0\}$. Thank to Theorem 13, we find $\eta_0 \eta_1 F^2 \leq \eta_0 \eta_1 \text{Tr}(P_1 \rho_0) \text{Tr}(P_1 \rho_1)$ or in other words $\eta_0 F^2 \leq \eta_0 \text{Tr}(P_1 \rho_0)$. We can also consider the USD POVM given by $\{E_? = P_0, E_0 = 0, E_1 = P_0^\perp\}$ and with Theorem 13, we have $\eta_0 \frac{F^2}{\text{Tr}(P_0 \rho_1)} \leq \eta_0$. Finally, we obtain $\eta_0 \text{Tr}(P_1 \rho_0) \leq Q_0 \leq \eta_0 \frac{F^2}{\text{Tr}(P_0 \rho_1)}$.

Next, we define the function $q(Q_0) = Q_0 + \frac{\eta_0 \eta_1 F^2}{Q_0}$ and minimize it under the constraint $\eta_0 \text{Tr}(P_1 \rho_0) \leq Q_0 \leq \eta_0 \frac{F^2}{\text{Tr}(P_0 \rho_1)}$. The resulting minimum will constitute a lower bound for Q . The function $q(Q_0)$ is convex ($\frac{d^2 q}{dQ_0^2}(Q_0) \geq 0$) and, therefore, it takes its minimum at the point Q_0^{\min} where the derivative vanishes ($\frac{dq}{dQ_0}(Q_0) = 0$) yielding $Q_0^{\min} = \sqrt{\eta_0 \eta_1} F$ or at the limits of the constraint interval ($Q_0^{\min} = \eta_0 \text{Tr}(P_1 \rho_0)$ and $Q_0^{\min} = \eta_0 \frac{F^2}{\text{Tr}(P_0 \rho_1)}$). That gives us the minimum of the function $q(Q_0)$ in three different regimes. In the first regime we have $q_{\min}(Q_0) = \eta_0 \text{Tr}(P_1 \rho_0) + \eta_1 \frac{F^2}{\text{Tr}(P_1 \rho_0)}$ and $Q_0^{\min} = \eta_0 \text{Tr}(P_1 \rho_0)$ if $\sqrt{\eta_0 \eta_1} F \leq \eta_0 \text{Tr}(P_1 \rho_0)$ that is to say if $\sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{\text{Tr}(P_1 \rho_0)}{F}$.

In the second regime we have $q_{\min}(Q_0) = 2\sqrt{\eta_0 \eta_1} F$ and $Q_0^{\min} = \sqrt{\eta_0 \eta_1} F$ if $\frac{\text{Tr}(P_1 \rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{F}{\text{Tr}(P_0 \rho_1)}$. The third regime gives $q_{\min}(Q_0) = \eta_0 \frac{F^2}{\text{Tr}(P_0 \rho_1)} + \eta_1 \text{Tr}(P_0 \rho_1)$ and $Q_0^{\min} = \eta_0 \frac{F^2}{\text{Tr}(P_0 \rho_1)}$ if $\frac{F}{\text{Tr}(P_0 \rho_1)} \leq \sqrt{\frac{\eta_1}{\eta_0}}$.

As a result we obtain lower bounds for the failure probability Q in three regimes as given in Eqn. (4.16). For each regime, the value of Q_0 which minimized $q(Q_0)$ is given and via Eqn. (4.23) we find the corresponding value that α has to take. We read off the values as $\alpha = \frac{\text{Tr}(P_1 \rho_0)}{F}$, $\alpha = \sqrt{\frac{\eta_1}{\eta_0}}$ and $\alpha = \frac{F}{\text{Tr}(P_0 \rho_1)}$ for the first, second and third regime, respectively. This completes the proof. ■

Let us note that, by construction, those bounds are tighter than the ones in chapter 2 [26]. Indeed, one could recover the three bounds in [26] by looking for the minimum of the function $q(Q_0)$ under the weaker constraints $\eta_0 F^2 \leq Q_0 \leq \eta_0$ as we will show in the last section of this chapter.

4.2 Parallel addition $\rho_0 \Sigma^{-1} \rho_1$

Before deriving the central theorem of this chapter and then provide the first class of exact solution for USD of two generic mixed states, we will first recall some useful results of linear algebra. We denote by M^{-1} the pseudo-inverse of a matrix M , which has not necessarily full rank. The pseudo-inverse can be defined via the singular-value decomposition of $M = UDV$ as $M^{-1} = UD^{-1}V$, where U and V are unitaries and D is a positive semi-definite and diagonal matrix. Whenever M is of full rank, the pseudo-inverse coincides with the inverse. In general, it is not known how to express the pseudo inverse of a sum $(A + B)^{-1}$ in terms of the pseudo inverses A^{-1} and B^{-1} [48, 49]. However, a related operation $A(A + B)^{-1}B$, called *parallel addition* and denoted by $A : B$ has been defined and studied in 1969 by Anderson and Duffin and will turn out useful in our context.

Lemma 3 [48] *Let A and B be two positive semi-definite matrices in M_n , then the support $\mathcal{S}_{A:B}$ of $A : B$ is given in terms of the supports of A and B as*

$$\mathcal{S}_{A:B} = \mathcal{S}_A \cap \mathcal{S}_B. \quad (4.29)$$

(See proof in Appendix C.)

Next let us recall the first reduction theorem for USD of mixed states (Theorem 9). We consider the problem of discriminating unambiguously two density matrices ρ_0 and ρ_1 with *a priori* probabilities η_0 and η_1 . We denote by r_0 the rank of ρ_0 and by r_1 the rank of ρ_1 . A general USD problem can satisfy $r_0 + r_1 \geq d$, where d is the dimension of the Hilbert space \mathcal{H} spanned by the two states. This means in particular that the two supports can overlap.

In the first reduction theorem it has been shown that any such USD problem can always be reduced to the one of discriminating ρ'_0 and ρ'_1 , two density matrices of rank r'_0 and r'_1 with *a priori* probabilities η'_0 and η'_1 , spanning the same Hilbert space \mathcal{H} of dimension $d = r'_0 + r'_1$. Indeed we can split off any common subspace of the supports $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1}$ to end up with $\mathcal{S}_{\rho'_0} \cap \mathcal{S}_{\rho'_1} = \{0\}$. As we have already seen, two supports do not overlap if and only if $\text{rank}(\rho'_0) + \text{rank}(\rho'_1) = \text{rank}(\rho'_0 + \rho'_1)$ holds. In such a reduced case, Lemma 3 implies $\mathcal{S}_{\rho'_0:\rho'_1} = 0$ that is to say $\rho'_0 : \rho'_1 = 0$.

We defining $\Sigma := \rho'_0 + \rho'_1$ to write the parallel addition as $\rho'_0 \Sigma^{-1} \rho'_1$. Since $\text{rank}(\rho'_0 + \rho'_1) = \dim(\mathcal{H})$, we end up with Σ having full rank and $\Sigma \Sigma^{-1} = \mathbb{1}_{\mathcal{H}}$. We therefore have the following corollary to Lemma 3,

Corollary 3 *Let ρ_0 and ρ_1 be two density matrices spanning a Hilbert space \mathcal{H} . Let Σ be the full rank operator defined as the sum of these two density matrices.*

$$\text{If } \mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\} \text{ then } \rho_0 \Sigma^{-1} \rho_1 = 0.$$

According to the first reduction theorem we can, without loss of generality, consider only USD problems of two density matrices without overlap of their supports. In the following, we consider two density matrices ρ_0 and ρ_1 (which are positive semi-definite matrices) such that $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ or equivalently $\text{rank}(\rho_0 + \rho_1) = \text{rank}(\rho_0) + \text{rank}(\rho_1) = \dim(\mathcal{H})$. As explained above, for such a problem, $\rho_0 \Sigma^{-1} \rho_1 = 0$, with $\Sigma = \rho_0 + \rho_1$ having full rank. This leads to

$$\rho_i = \rho_i \Sigma^{-1} \rho_i, \quad i = 0, 1 \quad (4.30)$$

since $\Sigma \Sigma^{-1} = \mathbb{1}_{\mathcal{H}}$. The projectors onto the supports of ρ_i , $i = 0, 1$, can then be written as

$$P_i = \sqrt{\rho_i} \Sigma^{-1} \sqrt{\rho_i}, \quad i = 0, 1 \quad (4.31)$$

To finish, let us precise that the two density matrices involved in a standard USD problem fulfill all the above properties since they do not overlap.

4.3 Necessary and sufficient conditions - first class of exact solutions

We are now ready to derive the main result of this chapter. The first part of this result gives compact necessary and sufficient conditions for a pair of mixed states to saturate the bounds of the failure probability \mathcal{Q} . The second part gives the corresponding POVMs in an explicit form.

Theorem 16 *Necessary and sufficient conditions to saturate the bounds on the failure probability*

Consider a USD problem defined by the two density matrices ρ_0 and ρ_1 and their respective a priori probabilities η_0 and η_1 such that their supports satisfy $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ (Any USD problem of two density matrices can be reduced to such a form according to Theorem 9). Let F_0 and F_1 be the two operators $\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. The fidelity F of the two states ρ_0 and ρ_1 is then given by $F = \text{Tr}(F_0) = \text{Tr}(F_1)$. We denote by P_0 and P_1 , the projectors onto the support of ρ_0 and ρ_1 . The optimal failure probability Q^{opt} for USD then satisfies

$$\begin{aligned} Q^{\text{opt}} &= \eta_1 \frac{F^2}{\text{Tr}(P_1\rho_0)} + \eta_0 \text{Tr}(P_1\rho_0) \Leftrightarrow \begin{cases} \rho_0 - \frac{\text{Tr}(P_1\rho_0)}{F} F_0 \geq 0 \\ \rho_1 - \frac{F}{\text{Tr}(P_1\rho_0)} F_1 \geq 0 \end{cases} \text{ for } \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{\text{Tr}(P_1\rho_0)}{F} \\ Q^{\text{opt}} &= 2\sqrt{\eta_0\eta_1}F \Leftrightarrow \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1 \geq 0 \end{cases} \text{ for } \frac{\text{Tr}(P_1\rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{F}{\text{Tr}(P_0\rho_1)} \\ Q^{\text{opt}} &= \eta_0 \frac{F^2}{\text{Tr}(P_0\rho_1)} + \eta_1 \text{Tr}(P_0\rho_1) \Leftrightarrow \begin{cases} \rho_0 - \frac{F}{\text{Tr}(P_0\rho_1)} F_0 \geq 0 \\ \rho_1 - \frac{\text{Tr}(P_0\rho_1)}{F} F_1 \geq 0 \end{cases} \text{ for } \frac{F}{\text{Tr}(P_0\rho_1)} \leq \sqrt{\frac{\eta_1}{\eta_0}} \end{aligned} \quad (4.32)$$

The POVM elements that realize these optimal failure probabilities, if the corresponding conditions are fulfilled, are given by

$$\begin{aligned} E_0 &= \Sigma^{-1} \sqrt{\rho_0} (\rho_0 - \alpha F_0) \sqrt{\rho_0} \Sigma^{-1} \\ E_1 &= \Sigma^{-1} \sqrt{\rho_1} \left(\rho_1 - \frac{1}{\alpha} F_1 \right) \sqrt{\rho_1} \Sigma^{-1} \\ E_? &= \Sigma^{-1} \left(\sqrt{\alpha} \sqrt{\rho_0} + \frac{1}{\sqrt{\alpha}} \sqrt{\rho_1} V^\dagger \right) F_0 \left(\sqrt{\alpha} \sqrt{\rho_0} + \frac{1}{\sqrt{\alpha}} V \sqrt{\rho_1} \right) \Sigma^{-1} \end{aligned} \quad (4.33)$$

with $\alpha = \frac{\text{Tr}(P_1\rho_0)}{F}$ for the first regime, $\alpha = \sqrt{\frac{\eta_1}{\eta_0}}$ for the second regime and $\alpha = \frac{F}{\text{Tr}(P_0\rho_1)}$ for the third regime and where the unitary operator V arises from a polar decomposition $\sqrt{\rho_0}\sqrt{\rho_1} = \sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}} V$.

Proof of Theorem 16 First, we give a proof for the necessary conditions.

Proof for the necessary conditions From Theorem 15 we know that the bounds on the failure probability are satisfied whenever $V^\dagger \sqrt{\rho_0} E_? = \alpha \sqrt{\rho_1} E_?$ with $\alpha = \frac{\text{Tr}(P_1\rho_0)}{F}$, $\alpha = \sqrt{\frac{\eta_1}{\eta_0}}$ and $\alpha = \frac{F}{\text{Tr}(P_0\rho_1)}$ for the three regimes, respectively.

We replace $E_?$ by $\mathbb{1} - E_0 - E_1$, multiply on the left by V and on the right by $\sqrt{\rho_0}$. This leads us to

$$\rho_0 - \alpha F_0 = \sqrt{\rho_0} E_0 \sqrt{\rho_0} \quad (4.34)$$

where we used the relation (4.13) $\sqrt{\rho_0} \sqrt{\rho_1} = F_0 V$ and the fact that the support of ρ_i and E_j are orthogonal for $i \neq j$. Indeed, in Lemma 1, we have seen that $\text{Tr}(E_i \rho_j) = 0 \Leftrightarrow E_i \rho_j = 0$ because E_i and ρ_j are positive semi-definite operators. The right hand side in (4.34) is positive semi-definite because of the form AA^\dagger with $A = \sqrt{\rho_0} \sqrt{E_0}$. Thus $\rho_0 - \alpha F_0$ must be positive semi-definite as well. A similar calculation where we multiply on the right by $\sqrt{\rho_1}$ instead of by $\sqrt{\rho_0}$ leads us to

$$\rho_1 - \frac{1}{\alpha} F_1 = \sqrt{\rho_1} E_1 \sqrt{\rho_1} \quad (4.35)$$

which is again a positive semi-definite operator.

With that we have proved that if equality holds in the bounds of Theorem 15 then we have

$$\begin{cases} \rho_0 - \alpha F_0 \geq 0 \\ \rho_1 - \frac{1}{\alpha} F_1 \geq 0 \end{cases} \quad (4.36)$$

which form, therefore, necessary conditions for equality in the bounds of Theorem 15.

Proof for the sufficient conditions Now we start with the assumption that the conditions (4.36) are fulfilled. Then we can construct an explicit POVM saturating the bound, therefore providing that the conditions are sufficient. Let us define the following POVM elements :

$$\begin{aligned} E_0 &= \Sigma^{-1} \sqrt{\rho_0} (\rho_0 - \alpha F_0) \sqrt{\rho_0} \Sigma^{-1} \\ E_1 &= \Sigma^{-1} \sqrt{\rho_1} \left(\rho_1 - \frac{1}{\alpha} F_1 \right) \sqrt{\rho_1} \Sigma^{-1} \\ E_? &= \Sigma^{-1} \left(\sqrt{\alpha} \sqrt{\rho_0} + \frac{1}{\sqrt{\alpha}} \sqrt{\rho_1} V^\dagger \right) F_0 \left(\sqrt{\alpha} \sqrt{\rho_0} + \frac{1}{\sqrt{\alpha}} V \sqrt{\rho_1} \right) \Sigma^{-1} \end{aligned} \quad (4.37)$$

First, let us verify that this is indeed a valid POVM. The three operators are positive semi-definite since they are of the form $A^\dagger M A$ where M is a positive semi-definite operator. In the first two cases this is true because of the conditions (4.36), in the third case it follows from the positivity of F_0 . The three operators sum to identity, $E_0 + E_1 + E_? = \mathbb{1}$, as can be checked by straightforward though lengthy calculation, making use of Eqn. (4.13). Next, we have to check that the given POVM is a valid USD POVM, that is, $\text{Tr}(\rho_0 E_1) = \text{Tr}(\rho_1 E_0) = 0$. This relation holds since the supports of ρ_0 and ρ_1 do not overlap. Therefore, corollary 3 applies and we have $\rho_0 \Sigma^{-1} \rho_1 = 0$ from which follows that $\sqrt{\rho_0} \Sigma^{-1} \rho_1 = 0$ and $\sqrt{\rho_1} \Sigma^{-1} \rho_0 = 0$. Finally, one can check in a straightforward though lengthy calculation, exploiting the properties used in the

previous checks that this POVM leads to the three desired failure probabilities. This completes the proof. ■

Let us first note that the assumption about the non-overlapping supports was only used to prove the sufficiency of the conditions. Their necessity does not require this assumption.

Moreover given a pair of two density matrices with their *a priori* probabilities, the middle regime does not always exists. A necessary condition for its existence is

$$\text{Tr}(P_1\rho_0)\text{Tr}(P_0\rho_1) \leq F^2 \quad (4.38)$$

as pointed out by Ulrike Herzog in [29].

To conclude the presentation of our first class of exact solutions, we would like to repeat that only the first reduction theorem is needed to derive Theorem 16. In chapter 6, we will provide pairs of density matrices that fall in this class as well as pairs of density matrices that are not included in it. It means that this class contains pairs of density matrices but does not cover all pairs.

4.4 The two pure states case revisited

It is possible to use Theorem 16 for two pure states $|\Psi_{\pm}\rangle$. We change here the label of the two states from '0/1' to '+/-' since one can always write two pure states $|\Psi_{\pm}\rangle = \alpha|0\rangle \pm \beta|1\rangle$ where α and β are real and such that $\alpha^2 + \beta^2 = 1$ in some suitable orthonormal basis $\{|0\rangle, |1\rangle\}$. For two pure states, the operators F_{\pm} are easy to explicit. Indeed $F_+ = F|\Psi_+\rangle\langle\Psi_+|$ and $F_- = F|\Psi_-\rangle\langle\Psi_-|$ with $F = |\langle\Psi_+|\Psi_-\rangle| = |2\alpha^2 - 1|$. Moreover one has the simple relation $\text{Tr}(P_+\rho_-) = \text{Tr}(P_-\rho_+) = F^2$.

The conditions in Theorem 16 then take the following form:

$$\begin{aligned} (1 - F^2)\rho_+ &\geq 0 \quad \text{for } \sqrt{\frac{\eta_-}{\eta_+}} \leq F \\ \left\{ \begin{array}{l} (1 - \sqrt{\frac{\eta_-}{\eta_+}}F)\rho_+ \geq 0 \\ (1 - \sqrt{\frac{\eta_+}{\eta_-}}F)\rho_- \geq 0 \end{array} \right. &\quad \text{for } F \leq \sqrt{\frac{\eta_-}{\eta_+}} \leq \frac{1}{F} \\ (1 - F^2)\rho_- &\geq 0 \quad \text{for } \frac{1}{F} \leq \sqrt{\frac{\eta_-}{\eta_+}} \end{aligned} \quad (4.39)$$

Since $(1 - \sqrt{\frac{\eta_-}{\eta_+}}F)$ and $(1 - \sqrt{\frac{\eta_+}{\eta_-}}F)$ for $\frac{1}{F} \leq \sqrt{\frac{\eta_-}{\eta_+}} \leq F$ range between 0 and F^2 , the constraints above are always fulfilled and our result reduces to that of Shimony and Jaeger. Moreover

we can give the POVM elements in a compact form thanks to the operator Σ^{-1} . The choice of our basis yields

$$\rho_{\pm} = \begin{pmatrix} \alpha^2 & \pm\alpha\beta \\ \pm\alpha\beta & \beta^2 \end{pmatrix} \quad (4.40)$$

such that

$$\Sigma^{-1} = \frac{1}{2} \begin{pmatrix} \alpha^{-2} & 0 \\ 0 & \beta^{-2} \end{pmatrix}. \quad (4.41)$$

It is therefore easy to write the optimal USD POVM as follows

$$E_+ = \frac{(1 - \alpha F)}{4} \begin{pmatrix} \alpha^{-2} & \frac{1}{\alpha\beta} \\ \frac{1}{\alpha\beta} & \beta^{-2} \end{pmatrix}, \quad (4.42)$$

$$E_- = \frac{(1 - \frac{F}{\alpha})}{4} \begin{pmatrix} \alpha^{-2} & \frac{-1}{\alpha\beta} \\ \frac{-1}{\alpha\beta} & \beta^{-2} \end{pmatrix} \quad (4.43)$$

and

$$E_? = \mathbb{1} - E_+ - E_- \quad (4.44)$$

with $\alpha = F$ for the first regime, $\alpha = \sqrt{\frac{\eta_-}{\eta_+}}$ for the second regime and $\alpha = \frac{1}{F}$ for the third regime. This expression of E_{\pm} leads naturally to the desired failure probability $Q^{\text{opt}} = F(\alpha\eta_+ + \frac{\eta_-}{\alpha})$ with the respective α s.

We can go beyond this remark and investigate under which conditions our bounds reduce to those given in chapter 2. The bounds derived by Rudolph *et al.* in [26] take the form

$$\begin{aligned} Q^{\text{opt}} &\geq \eta_1 + \eta_0 F^2 \text{ for } \sqrt{\frac{\eta_1}{\eta_0}} \leq F, \\ Q^{\text{opt}} &\geq 2\sqrt{\eta_0\eta_1}F \text{ for } F \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{F}, \\ Q^{\text{opt}} &\geq \eta_0 + \eta_1 F^2 \text{ for } \frac{1}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}}. \end{aligned} \quad (4.45)$$

Actually one can find Rudolph's bounds following the argumentation in the proof of Theorem 15 but using the weaker constraint $\eta_0 F^2 \leq Q_0 \leq \eta_0$. This means in particular that our bounds are tighter. To convince ourself, we can nevertheless consider our bounds and Rudolph's bounds in the five regimes of the ratio $\sqrt{\frac{\eta_1}{\eta_0}}$ given by

$$0 \leq F \leq \frac{\text{Tr}(P_1\rho_0)}{F} \leq \frac{F}{\text{Tr}(P_0\rho_1)} \leq \frac{1}{F}. \quad (4.46)$$

Note that this ordering is due to the Theorem 13 that tells us that $F \leq \frac{\text{Tr}(P_1\rho_0)}{F}$ since $F^2 \leq \text{Tr}(P_1\rho_0)$ and $\frac{F}{\text{Tr}(P_0\rho_1)} \leq \frac{1}{F}$ since $F^2 \leq \text{Tr}(P_0\rho_1)$. On the other hand, the inequality $\frac{\text{Tr}(P_1\rho_0)}{F} \leq \frac{F}{\text{Tr}(P_0\rho_1)}$ is not always fulfilled as we already discussed (see Eqn. (4.38)). We can now compare the two bounds in each regime.

In the middle regime given by $\frac{\text{Tr}(P_1\rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \text{Tr}(P_0\rho_1)$, the two bounds are equal. In the second regime given by $F \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{\text{Tr}(P_1\rho_0)}{F}$, Rudolph's bound still equals the overall lower bound $2\sqrt{\eta_0\eta_1}F$ and is therefore less or equal than our bound. In the third regime given by $\frac{F}{\text{Tr}(P_0\rho_1)} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{F}$, a similar argument holds: Rudolph's bound still equals the overall lower bound $2\sqrt{\eta_0\eta_1}F$ and is therefore less or equal than our bound.

In the outer regimes, things are a bit more subtle. We must again consider the function $q(Q_0) = Q_0 + \frac{\eta_0\eta_1F^2}{Q_0}$. This function decreases for $0 \leq Q_0 \leq \sqrt{\eta_0\eta_1}F$ and increases for $\sqrt{\eta_0\eta_1}F \leq Q_0$.

In the first regime, we have by definition $\sqrt{\frac{\eta_1}{\eta_0}} \leq F \leq \frac{\text{Tr}(P_1\rho_0)}{F}$ (See Eqn. (4.38)). We can multiply this inequality by η_0F to get $\sqrt{\eta_0\eta_1}F \leq \eta_0F^2 \leq \eta_0\text{Tr}(P_1\rho_0)$. For that range, $q(Q_0)$ increases so that $Q(\eta_0F^2) \leq Q(\eta_0\text{Tr}(P_1\rho_0))$ or in other words: $\eta_0F^2 + \eta_1 \leq \eta_0\text{Tr}(P_1\rho_0) + \eta_1\frac{F^2}{\text{Tr}(P_1\rho_0)}$.

In the fifth regime, we have $\frac{F}{\text{Tr}(P_0\rho_1)} \leq \frac{1}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}}$ (See Eqn.(4.50)). We can again multiply this inequality by η_0F to get $\eta_0\frac{F^2}{\text{Tr}(P_0\rho_1)} \leq \eta_0 \leq \sqrt{\eta_0\eta_1}F$. For that range, $q(Q_0)$ decreases so that $Q(\eta_0\frac{F^2}{\text{Tr}(P_0\rho_1)}) \geq Q(\eta_0)$ or in other words: $\eta_0\frac{F^2}{\text{Tr}(P_0\rho_1)} + \eta_1\text{Tr}(P_0\rho_1) \leq \eta_0 + \eta_1F^2$.

Since our bounds are tighter, Rudolph's bounds are reached if and only if, first, the conditions in Theorem 16 are fulfilled and, second, the equalities $\text{Tr}(P_0\rho_1) = \text{Tr}(P_1\rho_0) = F^2$ hold like in the pure state case. Let us now state the corresponding theorem and give the only part of the proof that changes with respect to theorems 15 and 16.

Theorem 17 *Necessary and sufficient conditions to saturate the bounds in [26]*

Consider a USD problem defined by the two density matrices ρ_0 and ρ_1 and their respective a priori probabilities η_0 and η_1 such that their supports satisfy $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ (Any USD problem of two density matrices can be reduced to such a form according to Theorem 9). Let F_0 and F_1 be the two operators $\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. The fidelity F of the two states ρ_0 and ρ_1 is then given by $F = \text{Tr}(F_0) = \text{Tr}(F_1)$. We denote by P_0 and P_1 , the projectors onto the support of ρ_0 and ρ_1 . The optimal failure probability Q^{opt} for USD then satisfies

$$\begin{aligned} Q^{\text{opt}} = \eta_1 + \eta_0 F^2 &\Leftrightarrow \begin{cases} \rho_0 - F F_0 \geq 0 \\ \rho_1 - \frac{1}{F} F_1 \geq 0 \end{cases} \quad \text{for } \sqrt{\frac{\eta_1}{\eta_0}} \leq F \\ Q^{\text{opt}} = 2\sqrt{\eta_0\eta_1}F &\Leftrightarrow \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1 \geq 0 \end{cases} \quad \text{for } F \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{F} \\ Q^{\text{opt}} = \eta_0 + \eta_1 F^2 &\Leftrightarrow \begin{cases} \rho_0 - \frac{1}{F} F_0 \geq 0 \\ \rho_1 - F F_1 \geq 0 \end{cases} \quad \text{for } \frac{1}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \end{aligned} \quad (4.47)$$

The POVM elements that realize these optimal failure probabilities, if the corresponding conditions are fulfilled, are given by

$$\begin{aligned} E_0 &= \Sigma^{-1} \sqrt{\rho_0} (\rho_0 - \alpha F_0) \sqrt{\rho_0} \Sigma^{-1} \\ E_1 &= \Sigma^{-1} \sqrt{\rho_1} \left(\rho_1 - \frac{1}{\alpha} F_1 \right) \sqrt{\rho_1} \Sigma^{-1} \\ E_? &= \Sigma^{-1} \left(\sqrt{\alpha} \sqrt{\rho_0} + \frac{1}{\sqrt{\alpha}} \sqrt{\rho_1} V^\dagger \right) F_0 \left(\sqrt{\alpha} \sqrt{\rho_0} + \frac{1}{\sqrt{\alpha}} V \sqrt{\rho_1} \right) \Sigma^{-1} \end{aligned} \quad (4.48)$$

with $\alpha = F$ for the first regime, $\alpha = \sqrt{\frac{\eta_1}{\eta_0}}$ for the second regime and $\alpha = \frac{1}{F}$ for the third regime and where the unitary operator V arises from a polar decomposition $\sqrt{\rho_0}\sqrt{\rho_1} = \sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}} V$.

In the first regime $\alpha = F$ implies that $E_1 = 0$. The resulting POVM has to be a projective measurement with projections onto the support of ρ_1 and onto its orthogonal complement, i.e. $E_0 = P_1^\perp$, $E_1 = 0$ and $E_? = P_1$. A direct proof from the explicit expressions in Eqn. (4.48) is difficult, however a simple reasoning allows to verify this statement. We consider only the non-trivial case where the supports of ρ_0 and ρ_1 are not identical. Of course, a two-element USD POVM satisfies $E_0 + E_? = \mathbb{1}$ with $\mathcal{S}_{E_0} \subset \mathcal{S}_{\rho_1}$. Then its structure must be such that $E_? = P_1 + R$ where P_1 is the projection onto the support of ρ_1 and R is an operator with support $\mathcal{S}_R \subset \mathcal{K}_{\rho_1}$ which satisfies $E_0 + R = P_1^\perp$. Then it follows that $Q = \eta_1 + \eta_0 \text{Tr}(P_1 \rho_0) + \eta_0 \text{Tr}(R \rho_0)$. In our non-trivial case we will have $\text{Tr}(R \rho_0) > 0$ as soon as $R \neq 0$. Therefore we find as an optimal

solution within this class of two-element USD POVM, the POVM with $R = 0$ leading to $E_? = P_1$ and $E_0 = P_1^\perp$. We can actually write the failure probability as $Q^{\text{opt}} = \eta_1 + \eta_0 F^2$. Indeed $\rho_1 = \frac{1}{F} F_1$ then $\rho_1^2 = \frac{1}{F^2} \sqrt{\rho_1} \rho_0 \sqrt{\rho_1}$. This implies $F^2 \rho_1 = P_1 \rho_0 P_1$ and finally $\text{Tr}(P_1 \rho_0) = F^2$. This is consistent with the results derived above and gives the correct failure probability. In the third regime, we have $\alpha = \frac{1}{F}$. Therefore $E_0 = 0$ and the corresponding POVM is a projective measurement with $E_0 = 0$, $E_1 = P_0^\perp$, $E_? = P_0$.

Proof of Theorem 17 We will only derive the three minima of the function $q(Q_0) = Q_0 + \frac{\eta_0 \eta_1 F^2}{Q_0}$ since the remaining part of the proof does not change (the proof correspond to Theorem 15 where the bounds are derived). Here we consider weaker range constraints on Q_0 and Q_1 : $0 \leq Q_0 \leq \eta_0$ and $0 \leq Q_1 \leq \eta_1$. We then minimize $q(Q_0)$ under the constraint $\eta_0 F^2 \leq Q_0 \leq \eta_0$. Again, the function $q(Q_0)$ is convex ($\frac{d^2 q}{dQ_0^2}(Q_0) \geq 0$) and, therefore, it takes its minimum at the point Q_0^{\min} where the derivative vanishes ($\frac{dq}{dQ_0}(Q_0) = 0$) yielding $Q_0^{\min} = \sqrt{\eta_0 \eta_1} F$ or at the limits of the constraint interval ($Q_0^{\min} = \eta_0 F^2$ and $Q_0^{\min} = \eta_0$). That gives us the minimum of the function $q(Q_0)$ in three different regimes. In the first regime we have $q_{\min}(Q_0) = \eta_0 F^2 + \eta_1$ and $Q_0^{\min} = \eta_0 F^2$ if $\sqrt{\eta_0 \eta_1} F \leq \eta_0 F^2$ that is to say if $\sqrt{\frac{\eta_1}{\eta_0}} \leq F$. In the second regime we have $q_{\min}(Q_0) = 2\sqrt{\eta_0 \eta_1} F$ and $Q_0^{\min} = \sqrt{\eta_0 \eta_1} F$ if $F \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{F}$. The third regime gives $q_{\min}(Q_0) = \eta_0 + \eta_1 F^2$ and $Q_0^{\min} = \eta_0$ if $\frac{1}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}}$.

As a result we obtain lower bounds for the failure probability Q in three regimes as given in Eqn. (4.47). Since $Q_0 = \alpha \eta_0 F$, we read off the values of α as $\alpha = F$, $\alpha = \sqrt{\frac{\eta_1}{\eta_0}}$ and $\alpha = \frac{1}{F}$ for the first, second and third regime, respectively. This completes the proof. ■

In the next chapter, we will derive a second class of exact solutions. This class is concerned with pairs of geometrically uniform states in four dimensions.

Chapter 5

Second class of exact solutions

In this chapter, we derive three important results. First we derive a theorem concerned with the rank of an optimal USD measurement. Next, we propose a corollary which is interested in the spectrum of an optimal USD measurement. Finally we give the main result of this chapter, a second class of exact solutions. This class corresponds to any pair of *geometrically uniform* states in four dimensions. To be proved, this result requires most of the theorems previously derived in this thesis.

5.1 Overall lower bound and rank of the POVM elements

The maximum rank $r_{E_i}^{max}$ of a USD POVM element E_i , $i = 0, 1$ is

$$r_{E_0}^{max} = \dim(\mathcal{K}_{\rho_1}), \quad (5.1)$$

$$r_{E_1}^{max} = \dim(\mathcal{K}_{\rho_0}). \quad (5.2)$$

$$(5.3)$$

In the case where $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$, the *maximum rank* of the USD POVM elements E_i , $i = 0, 1$ is $\dim(\mathcal{S}_{\rho_i})$, the rank of the mixed states ρ_i . Indeed E_i has support in \mathcal{K}_{ρ_j} , $i, j = 0, 1$, $j \neq i$ and therefore, if $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$,

$$\text{rank}(E_i) \leq \dim(\mathcal{K}_{\rho_j}) \quad (5.4)$$

$$\leq \dim(\mathcal{H}) - \dim(\mathcal{S}_{\rho_j}) \quad (5.5)$$

$$\leq \dim(\mathcal{S}_{\rho_0}) + \dim(\mathcal{S}_{\rho_1}) - \dim(\mathcal{S}_{\rho_j}) \quad (5.6)$$

$$\leq \dim(\mathcal{S}_{\rho_i}), \quad i = 0, 1. \quad (5.7)$$

Note that in Chapter 3, we already proved that

$$r_{E_2}^{max} = \min(\dim(\mathcal{S}_{\rho_0}), \dim(\mathcal{S}_{\rho_1})). \quad (5.8)$$

The first theorem of this chapter states that the two POVM elements E_0 and E_1 of an optimal USD both have *maximum rank* only if the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1$ are positive semi-definite. The attentive reader can recognize the two operators involved in the middle regime of Theorem 16.

Theorem 18 *Rank of E_0 and E_1*

Consider a USD problem defined by two density matrices ρ_0 and ρ_1 and their respective a priori probabilities η_0 and η_1 such that their supports satisfy $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ (Any USD problem of two density matrices can be reduced to such a form according to Theorem 9). Consider also an optimal measurement $\{E_0^{opt}, E_1^{opt}, E_2^{opt}\}$ to that problem. Let F_0 and F_1 be the two operators $\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. The fidelity F of the two states ρ_0 and ρ_1 is then given by $F = \text{Tr}(F_0) = \text{Tr}(F_1)$.

If the two POVM elements E_0^{opt} and E_1^{opt} have maximal rank $\dim(\mathcal{S}_{\rho_0})$ and $\dim(\mathcal{S}_{\rho_1})$, respectively, then

$$\begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1 \geq 0. \end{cases} \quad (5.9)$$

Proof We consider an optimal measurement for unambiguously discriminating two mixed states ρ_0 and ρ_1 . We can therefore use the necessary and sufficient conditions derived by Eldar [36]. We recall them here. Necessary and sufficient conditions for a measurement $\{E_k\}$, $k = ?, 0, 1$ to be optimal are that there exists $Z \geq 0$ such that

$$ZE_? = 0, \quad (5.10)$$

$$E_0(Z - \eta_0\rho_0)E_0 = 0, \quad (5.11)$$

$$E_1(Z - \eta_1\rho_1)E_1 = 0, \quad (5.12)$$

$$P_1^\perp(Z - \eta_0\rho_0)P_1^\perp \geq 0, \quad (5.13)$$

$$P_0^\perp(Z - \eta_1\rho_1)P_0^\perp \geq 0. \quad (5.14)$$

If E_0 and E_1 have *maximum rank* and Eqn. (5.11) and Eqn. (5.12) are fulfilled then the two Hermitian operators $P_1^\perp(Z - \eta_0\rho_0)P_1^\perp$ and $P_0^\perp(Z - \eta_1\rho_1)P_0^\perp$ must vanish. Indeed the situation is the following. We consider two positive operators A and B , with A full rank and $ABA^\dagger = 0$. We can see this relation as of the form $CC^\dagger = 0$ with $C = A\sqrt{B}$. Moreover, such an equation $CC^\dagger = 0$ is equivalent to $C = 0$ for any matrix C (See Appendix A for a proof of this statement). Consequently, $ABA^\dagger = 0$ is equivalent to $A\sqrt{B} = 0$. Finally, since A is full rank A^{-1} exists and B must vanish.

In Eqn. (5.11) and (5.13), we have $A = E_0$ and $B = P_1^\perp(Z - \eta_0\rho_0)P_1^\perp$. In Eqn. (5.12) and (5.14), we have $A = E_1$ and $B = P_0^\perp(Z - \eta_1\rho_1)P_0^\perp$. As a result, $P_1^\perp(Z - \eta_0\rho_0)P_1^\perp$ and $P_0^\perp(Z - \eta_1\rho_1)P_0^\perp$ must vanish if E_0 and E_1 have maximum rank. Finally to prove the statement of the theorem we can show the following equivalence:

$$\exists Z \geq 0 \text{ such that } \begin{cases} ZE_i = 0 \\ P_0^\perp(Z - \eta_1\rho_1)P_0^\perp = 0 \\ P_1^\perp(Z - \eta_0\rho_0)P_1^\perp = 0 \end{cases} \Leftrightarrow \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1 \geq 0 \end{cases} \quad (5.15)$$

where $P_0^\perp(Z - \eta_1\rho_1)P_0^\perp$ and $P_1^\perp(Z - \eta_0\rho_0)P_1^\perp$ are positive semi-definite operators. To prove this statement, we proceed by equivalence.

Since the two supports do not overlap, we can make use of the full rank operator $\Sigma^{-1} = (\rho_0 + \rho_1)^{-1}$ introduced in chapter 4. Let us repeat here that its main property is

$$\rho_i \Sigma^{-1} \rho_j = \rho_i \delta_{ij}, \quad i = 0, 1. \quad (5.16)$$

As a consequence, we get the interesting relations

$$\rho_0 \Sigma^{-1} = \rho_0 \Sigma^{-1} P_1^\perp, \quad (5.17)$$

$$P_1^\perp \rho_0 \Sigma^{-1} = P_1^\perp. \quad (5.18)$$

Indeed $\rho_0 \Sigma^{-1} = \rho_0 \Sigma^{-1} (P_1 + P_1^\perp) = \rho_0 \Sigma^{-1} \rho_1 \rho_1^{-1} + \rho_0 \Sigma^{-1} P_1^\perp = \rho_0 \Sigma^{-1} P_1^\perp$. Moreover, $P_1^\perp = P_1^\perp \mathbb{1} = P_1^\perp (\rho_0 + \rho_1) \Sigma^{-1} = P_1^\perp \rho_0 \Sigma^{-1}$. The same relations are of course true when we swap 0 and 1.

$$\rho_1 \Sigma^{-1} = \rho_1 \Sigma^{-1} P_0^\perp, \quad (5.19)$$

$$P_0^\perp \rho_1 \Sigma^{-1} = P_0^\perp. \quad (5.20)$$

It follows that the two equalities $P_1^\perp(Z - \eta_0\rho_0)P_1^\perp = 0$ and $P_0^\perp(Z - \eta_1\rho_1)P_0^\perp = 0$ are equivalent to $\rho_0 \Sigma^{-1} (Z - \eta_0\rho_0) \Sigma^{-1} \rho_0 = 0$ and $\rho_1 \Sigma^{-1} (Z - \eta_1\rho_1) \Sigma^{-1} \rho_1 = 0$. Hence the assertion

$$\exists Z \geq 0 \text{ such that } \begin{cases} ZE_i = 0 \\ P_0^\perp(Z - \eta_1\rho_1)P_0^\perp = 0 \\ P_1^\perp(Z - \eta_0\rho_0)P_1^\perp = 0 \end{cases} \quad (5.21)$$

can be replaced by

$$\exists Z \geq 0 \text{ such that } \begin{cases} ZE_i = 0 \\ \rho_i \Sigma^{-1} Z \Sigma^{-1} \rho_i = \eta_i \rho_i, \text{ for } i = 0, 1. \end{cases} \quad (5.22)$$

Since the operator Z is positive, we know it exists an operator Y such that $Z = YY^\dagger$. We can insert it in $\rho_i \Sigma^{-1} Z \Sigma^{-1} \rho_i = \eta_i \rho_i$ and find that it exists W_i , a unitary transformation such that

$$W_i^\dagger Y^\dagger \Sigma^{-1} \rho_i = \sqrt{\eta_i} \sqrt{\rho_i}, \quad i = 0, 1. \quad (5.23)$$

Moreover, Σ is full rank. As a result we can decompose Z as $Z = \rho_0 \Sigma^{-1} Z \Sigma^{-1} \rho_0 + \rho_0 \Sigma^{-1} Z \Sigma^{-1} \rho_1 + \rho_1 \Sigma^{-1} Z \Sigma^{-1} \rho_0 + \rho_1 \Sigma^{-1} Z \Sigma^{-1} \rho_1$. This directly yields

$$\begin{aligned} Z &= \eta_0 \rho_0 + \eta_1 \rho_1 + \sqrt{\eta_0 \eta_1} \sqrt{\rho_0} W_0^\dagger W_1 \sqrt{\rho_1} + \sqrt{\eta_0 \eta_1} \sqrt{\rho_1} W_1^\dagger W_0 \sqrt{\rho_0} \\ &= (\sqrt{\eta_0} \sqrt{\rho_0} W_0^\dagger W_1 + \sqrt{\eta_1} \sqrt{\rho_1}) (\sqrt{\eta_0} W_1^\dagger W_0 \sqrt{\rho_0} + \sqrt{\eta_1} \sqrt{\rho_1}) \end{aligned} \quad (5.24)$$

We finally read off Y^\dagger as

$$Y^\dagger = \sqrt{\eta_0} W^\dagger \sqrt{\rho_0} + \sqrt{\eta_1} \sqrt{\rho_1} \quad (5.25)$$

where $W^\dagger = W_1^\dagger W_0$.

We now make use of the relation $ZE_\gamma = 0$ which is equivalent to $Y^\dagger E_\gamma = 0$ since $AA^\dagger = 0 \Leftrightarrow A = 0$ for any matrix A . We can explicitly write $Y^\dagger E_\gamma = 0$ with $Y^\dagger = \sqrt{\eta_0} W^\dagger \sqrt{\rho_0} + \sqrt{\eta_1} \sqrt{\rho_1}$ and $W = W_0^\dagger W_1$. This leads to the statement

$$\exists Y, W \text{ such that } \begin{cases} WW^\dagger = \mathbb{1}, \\ YY^\dagger = Z, \\ -\sqrt{\eta_0} W^\dagger \sqrt{\rho_0} E_\gamma = \sqrt{\eta_1} \sqrt{\rho_1} E_\gamma. \end{cases} \quad (5.26)$$

In fact, this relation $-\sqrt{\eta_0} W^\dagger \sqrt{\rho_0} E_\gamma = \sqrt{\eta_1} \sqrt{\rho_1} E_\gamma$ is only possible when $-W$ is a unitary transformation coming from a polar decomposition of $\sqrt{\rho_0} \sqrt{\rho_1}$ otherwise theorem 13 in chapter 4 is violated. Indeed theorem 13 tells us that the product between Q_0 and Q_1 is lower bounded as

$$Q_0 Q_1 \geq \eta_0 \eta_1 F^2 \quad (5.27)$$

where the equality holds if and only if a unitary operator V arising from a polar decomposition

$$\sqrt{\rho_0} \sqrt{\rho_1} = \sqrt{\sqrt{\rho_0} \rho_1 \sqrt{\rho_0}} V \quad (5.28)$$

satisfies

$$V^\dagger \sqrt{\rho_0} \sqrt{E_\gamma} = \alpha \sqrt{\rho_1} \sqrt{E_\gamma} \quad (5.29)$$

for some $\alpha \in \mathbb{R}^+$. Moreover $F = \max_U |\text{Tr}(U^\dagger \sqrt{\rho_0} \sqrt{\rho_1})|$ is reached only for unitaries U coming from a polar decomposition of $\sqrt{\rho_0} \sqrt{\rho_1}$. For any unitary V which does not come from a polar decomposition, we then have the strict inequality $F > |\text{Tr}(V^\dagger \sqrt{\rho_0} \sqrt{\rho_1})|$. In other words, if V does not come from a polar decomposition then

$$\eta_0 \eta_1 F^2 > \eta_0 \eta_1 |\text{Tr}(V^\dagger \sqrt{\rho_0} \sqrt{\rho_1})|. \quad (5.30)$$

Moreover, since $V^\dagger \sqrt{\rho_0} \sqrt{E_?} = \alpha \sqrt{\rho_1} \sqrt{E_?}$, the Cauchy-Schwarz (in)equality tells us that

$$Q_0 Q_1 = \eta_0 \eta_1 \text{Tr}(E_? \rho_0) \text{Tr}(E_? \rho_1) \quad (5.31)$$

$$= \eta_0 \eta_1 |\text{Tr}(V^\dagger \sqrt{\rho_0} E_? \sqrt{\rho_1})| \quad (5.32)$$

$$= \eta_0 \eta_1 |\text{Tr}(V^\dagger \sqrt{\rho_0} \sqrt{\rho_1})|. \quad (5.33)$$

Consequently $\eta_0 \eta_1 F^2 > Q_0 Q_1$ and the theorem 13 is violated. This implies that $-W$ comes from a polar decomposition of $\sqrt{\rho_0} \sqrt{\rho_1}$. At that point, we simply use the equivalence derived in chapter 4

$$-\sqrt{\eta_0} W^\dagger \sqrt{\rho_0} E_? = \sqrt{\eta_1} \sqrt{\rho_1} E_? \Leftrightarrow \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1 \geq 0. \end{cases} \quad (5.34)$$

Indeed Theorem 13 tells us that, for any $-W$ coming from a polar decomposition of $\sqrt{\rho_0} \sqrt{\rho_1}$,

$$-\sqrt{\eta_0} W^\dagger \sqrt{\rho_0} E_? = \sqrt{\eta_1} \sqrt{\rho_1} E_? \Leftrightarrow Q^{\text{opt}} = 2\sqrt{\eta_0 \eta_1} F. \quad (5.35)$$

And Theorem 16 says that, for any $-W$ coming from a polar decomposition of $\sqrt{\rho_0} \sqrt{\rho_1}$,

$$Q^{\text{opt}} = 2\sqrt{\eta_0 \eta_1} F \Leftrightarrow \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1 \geq 0. \end{cases} \quad (5.36)$$

This completes the proof. ■

There are at least three consequences to the theorem above. First, it indicates that an optimal POVM is, in general, unlikely to have its elements E_0 and E_1 of maximum rank. This comes from the fact that the positivity of two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1$ is only possible the middle regime defined by $\frac{\text{Tr}(P_1 \rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{F}{\text{Tr}(P_0 \rho_1)}$. Second, we can use Theorem 18 to investigate further the spectrum of an optimal USDM. Last but not least, we can derive a new class of exact solutions for the problem of unambiguously discriminating two mixed states.

5.2 Maximum rank and *a priori* probabilities

Theorem 18 can be rephrased as

$$\text{If } \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1 \geq 0 \end{cases} \text{ is violated then } \begin{cases} \text{rank}(E_0) < \dim(\mathcal{S}_{\rho_0}) \\ \text{or} \\ \text{rank}(E_1) < \dim(\mathcal{S}_{\rho_1}). \end{cases} \quad (5.37)$$

In this section, we discuss why Theorem 18 suggests that E_0 and E_1 have maximum rank only in a small regime of the ratio between the two *a priori* probabilities around 1.

We already know that the positivity conditions in (5.37) are quite restrictive since they are reachable only in the middle regime of the ratio $\sqrt{\frac{\eta_1}{\eta_0}}$. Indeed we repeat here that

$$Q^{\text{opt}} = 2\sqrt{\eta_0\eta_1}F \Leftrightarrow \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1 \geq 0 \end{cases} \text{ for } \frac{\text{Tr}(P_1\rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{F}{\text{Tr}(P_0\rho_1)} \quad (5.38)$$

where $Q^{\text{opt}} = 2\sqrt{\eta_0\eta_1}F$ is an overall lower bound on the failure probability that cannot be reached in the two outer regimes.

Second, the boundaries of this middle regime can actually be made tighter. Indeed the three regimes of the ratio $\sqrt{\frac{\eta_1}{\eta_0}}$ where built considering some constraints on Q_0 and Q_1 . Stronger constraints means tighter boundaries and the constraints on Q_0 and Q_1 could in principle be made stronger if more knowledge on the two density matrices ρ_0 and ρ_1 is provided.

Let us give such an example of stronger constraints on Q_0 for, say, a POVM having the symmetry $E_1 = UE_0U$ where U is a unitary transformation¹.

Since $E_0 \subset \mathcal{K}_{\rho_1}$, there exists $R \geq 0$ in \mathcal{K}_{ρ_1} such that $E_1 + E_? = P_1 + R$. Moreover the POVM element $E_?$ is invariant under U since $UE_?U = U(\mathbb{1} - E_0 - E_1)U = (\mathbb{1} - E_1 - E_0) = E_?$. Hence, $E_0 + E_? = U(E_1 + E_?)U = P_0 + URU$. We therefore obtain the trace equality

$$\text{Tr}(E_?) = 2\text{Tr}(R). \quad (5.39)$$

Indeed $\text{Tr}(E_1 + E_?) = \text{Tr}(P_1) + \text{Tr}(R)$ and $\text{Tr}(E_0 + E_?) = \text{Tr}(P_0) + \text{Tr}(R)$ so that $\text{Tr}(\mathbb{1}) + \text{Tr}(E_?) = \text{Tr}(P_0) + \text{Tr}(P_1) + 2\text{Tr}(R)$. And, for a standard USD problem, the equality $\text{Tr}(\mathbb{1}) = \text{Tr}(P_0) + \text{Tr}(P_1)$ holds.

We can now consider Q_0 . $E_1 + E_? = P_1 + R$ and $\text{Tr}(E_1\rho_0) = 0$, we can consequently write

$$Q_0 = \eta_0\text{Tr}(E_?\rho_0) \quad (5.40)$$

$$= \eta_0\text{Tr}(E_?\rho_0) + \eta_0\text{Tr}(E_1\rho_0) \quad (5.41)$$

$$= \eta_0\text{Tr}(P_1\rho_0) + \eta_0\text{Tr}(R\rho_0). \quad (5.42)$$

The operator $P_1^\perp\rho_0P_1^\perp$ is a positive semi-definite operator so that its eigenvalues are all positive or equal to 0. We can here introduce λ_{\min} , its smallest non vanishing eigenvalue. It follows that

¹We will see in the next section that such a symmetry is possible for USD of two geometrically uniform states.

$Q_0 \geq \eta_0 \text{Tr}(P_1 \rho_0) + \eta_0 \text{Tr}(R) \lambda_{\min}$. Together with Eqn.(5.39) this yields

$$Q_0 \geq \eta_0 \text{Tr}(P_1 \rho_0) + \frac{\eta_0 \lambda_{\min}}{2} \text{Tr}(E_?) \quad (5.43)$$

$$\geq \eta_0 \text{Tr}(P_1 \rho_0) + \frac{\eta_0 \lambda_{\min}}{2} \text{Tr}(E_? \rho_0). \quad (5.44)$$

In other words, for any USD POVM such that $E_1 = U E_0 U$ where U is a unitary transformation,

$$Q_0 \geq \frac{\eta_0 \text{Tr}(P_1 \rho_0)}{1 - \lambda_{\min}/2} \quad (5.45)$$

where $\lambda_{\min} = \min\{\text{Spec}(P_1^\perp \rho_0 P_1^\perp)\}$. It becomes clear that with more knowledge on the mixed states ρ_0 and ρ_1 , we could make the boundaries of the middle regime tighter. The extreme case would be a middle regime reduced to $\sqrt{\frac{\eta_1}{\eta_0}} = 1$. These considerations might indicate that, in general, E_0 and E_1 have *maximum rank* only for some range of the ratio between the *a priori* probabilities around $\eta_1 = \eta_0 = 1/2$.

5.3 A fourth, incomplete, reduction theorem

In the case where $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$, the *maximum rank* of the USD POVM elements E_i , $i = 0, 1$ is r_i , the rank of the mixed states ρ_i . Moreover if not only $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ but also $\mathcal{K}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ and $\mathcal{K}_{\rho_1} \cap \mathcal{S}_{\rho_0} = \{0\}$ then ρ_0 and ρ_1 have the same rank r in a $2r$ -dimensional Hilbert space and we end up with

$$r_{E_i}^{\max} = r, i = 0, 1, ? \quad (5.46)$$

One can actually use Theorem 18 to study the spectrum of the elements of an optimal USDM. In fact, we can state that, for a standard USD problem, if $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1$ are not positive semi-definite then the optimal measurement is such that $E_?$ possesses one eigenvalue equal to 1 and E_0 or E_1 too. Let us make this result precise in the following theorem.

Corollary 4 *A fourth, incomplete, reduction Theorem*

Consider a standard USD problem defined by two density matrices ρ_0 and ρ_1 and their respective a priori probabilities η_0 and η_1 (any USD problem of two density matrices can be reduced to such a form according to Chapter 3). Consider also an optimal measurement $\{E_0^{opt}, E_1^{opt}, E_2^{opt}\}$ to that problem. Let F_0 and F_1 be the two operators $\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. The fidelity F of the two states ρ_0 and ρ_1 is then given by $F = \text{Tr}(F_0) = \text{Tr}(F_1)$.

$$\text{If } \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1 \geq 0 \end{cases} \text{ is violated then there exists} \quad (5.47)$$

$$|e\rangle \in \mathcal{S}_{\rho_0} \text{ and } |e'\rangle \in \mathcal{K}_{\rho_0} \text{ such that } \begin{cases} E_2^{opt}|e\rangle = |e\rangle \\ E_1^{opt}|e'\rangle = |e'\rangle \\ E_0^{opt}|e\rangle = E_0^{opt}|e'\rangle = E_1^{opt}|e\rangle = E_2^{opt}|e'\rangle = 0, \end{cases}$$

or

$$|e\rangle \in \mathcal{S}_{\rho_1} \text{ and } |e'\rangle \in \mathcal{K}_{\rho_1} \text{ such that } \begin{cases} E_2^{opt}|e\rangle = |e\rangle \\ E_0^{opt}|e'\rangle = |e'\rangle \\ E_1^{opt}|e\rangle = E_1^{opt}|e'\rangle = E_0^{opt}|e\rangle = E_2^{opt}|e'\rangle = 0. \end{cases}$$

First let us note that this theorem makes this assumption of a *standard* USD problem. It is in principle not necessary to make such an assumption to derive the existence of some eigenvector of E_2 , E_0 or E_1 with eigenvalue 1 since Theorem 18 is valid for any pair of density matrices without overlapping supports. Nevertheless, this theorem aims to be a 'fourth' reduction theorem. It means in particular that, for any given USD problem of two density matrices, we would like to apply our 'four' reduction theorems and always end up with the optimal USD measurement.

The above theorem is a kind of incomplete *reduction theorem*. A reduction theorem is a theorem that allows us to decrease the size of the USD problem by splitting off some subspace onto which no optimization is needed. To have a complete reduction theorem here, we would need to characterize $|e\rangle$ and $|e'\rangle$ without solving the whole optimization problem. But only the existence of $|e\rangle$ and $|e'\rangle$ is so far ensured. If such a reduction theorem were found then we would have a recipe to solve any USD problem. Let us assume that $|e\rangle$ and $|e'\rangle$ are fully characterized and let us start from a general USD of two mixed states. We use the three first reduction theorems to make it standard. We then check whether the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1$ are positive semi-definite. If yes then we know the optimal failure probability

as well as the optimal measurement to perform since this case falls into the first class of exact solutions (middle regime). If the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1$ are not positive semi-definite, we can use our last reduction theorem to get rid of two dimensions. At that point, we check again the positivity of the two operators $\rho'_0 - \sqrt{\frac{\eta'_1}{\eta'_0}} F'_0$ and $\rho'_1 - \sqrt{\frac{\eta'_0}{\eta'_1}} F'_1$ of the reduced problem. We see here a constructive way to solve any USD problem. If the two operators $\rho'_0 - \sqrt{\frac{\eta'_1}{\eta'_0}} F'_0$ and $\rho'_1 - \sqrt{\frac{\eta'_0}{\eta'_1}} F'_1$ never happen to be positive, we end up with only two pure states and can finally find the optimal measurement (see Fig. 5.1). The only problem in that nice picture is that we only know that $|e\rangle$ and $|e'\rangle$ exist but we cannot until now characterize them.

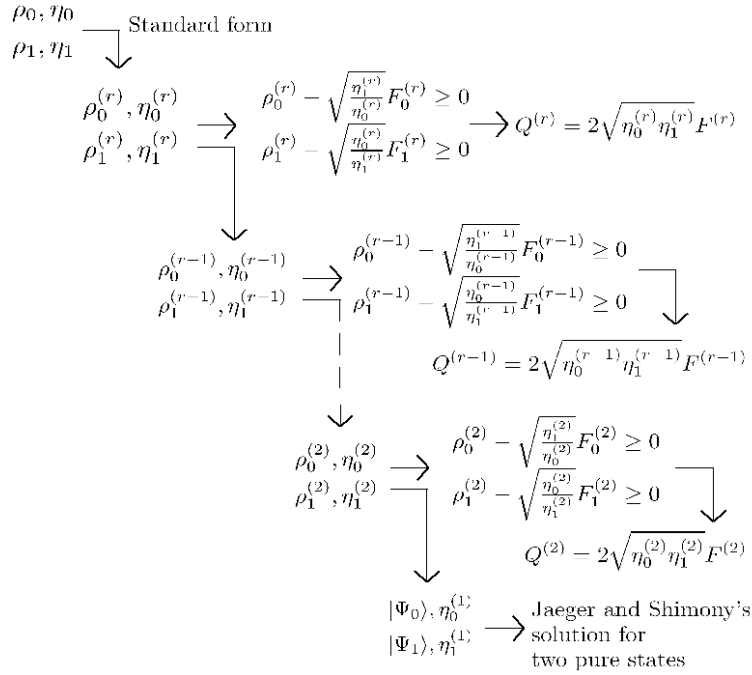


Figure 5.1: A constructive way to solve any USD problem (the exponent $^{(r)}$ denotes the rank of the density matrices after reduction)

Here comes another important remark. There are only two ways to find a complete characterization of the two eigenvectors $|e\rangle$ and $|e'\rangle$. The first is to consider a low dimensional USD problem. The second is to consider a highly symmetric problem. The former case simply is the two pure states case. Indeed, either the operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1$ are positive semi-definite or we have $|e\rangle \in \mathcal{S}_{\rho_{0/1}}$ and $|e'\rangle \in \mathcal{K}_{\rho_{0/1}}$, eigenvectors of $E_?$ and $E_{1/0}$. In only two dimensions, there is no freedom and $|e\rangle$ and $|e'\rangle$ must be $|\Psi_{0/1}\rangle$ and $|\Psi_{0/1}^\perp\rangle$. If we are interested in higher dimensions, we use some symmetry to give us enough constraint to fully characterize

$|e\rangle$ and $|e'\rangle$, we can go up to four dimensions. This is the object of our last section. Before that let us prove Corollary 4.

Proof of Corollary 4 To prove this corollary, we begin with the statement given in Theorem 18 for two density matrices ρ_0 and ρ_1 with same rank n in a $2n$ -dimensional Hilbert space. The maximum rank of E_0 and E_1 then equal n . Let us for example consider that $\text{rank}(E_0) < n$. The other option corresponding to $\text{rank}(E_1) < n$ follows the same argumentation. Because of the completeness relation $E_? + E_1 + E_0 = \mathbb{1}$ fulfilled by the POVM elements, we have, onto the subspace \mathcal{S}_{P_0} , the following equality $P_0 E_? P_0 + P_0 E_1 P_0 + P_0 E_0 P_0 = P_0$. However, $\mathcal{S}_{E_1} \in \mathcal{S}_{P_0}^\perp$ so that we are left with

$$P_0 E_? P_0 + P_0 E_0 P_0 = P_0. \quad (5.48)$$

Furthermore, in $P_0 E_0 P_0$'s eigenbasis, we have $P_0 E_0 P_0 = \sum_{i=1}^{n-1} \lambda_i |\lambda_i\rangle \langle \lambda_i|$ since E_0 is of rank $n-1$ and $P_0 = \sum_{i=1}^{n-1} |\lambda_i\rangle \langle \lambda_i| + |e\rangle \langle e|$ where $|e\rangle$ completes the n dimensional orthogonal basis of \mathcal{S}_{P_0} . As a result, $E_? |e\rangle = (\mathbb{1} - E_0 - E_1) |e\rangle = |e\rangle - 0 - 0$ and $|e\rangle$ is an eigenvector of $E_?$ with eigenvalue 1.

We can actually go one step further. Since the completeness relation is already fulfilled onto the subspace spanned by $|e\rangle$ and $|e'\rangle$, no optimization is required onto it and we can split it off from the original USD problem. The remaining USD problem to optimize concerns ρ'_0 and ρ'_1 originated respectively from the density matrix ρ_0 and ρ_1 . Moreover, ρ'_0 has rank $n-1$ while ρ'_1 has rank n . We can indeed denote by $\mathcal{S}_{|e\rangle}$ the subspace spanned by $|e\rangle$. The reduced Hilbert space is $\mathcal{H} / \mathcal{S}_{|e\rangle}$ and \mathcal{S}_{ρ_0} , the support of ρ_0 , loses one dimension. Thanks to the second reduction theorem, we can reduce this problem to the one of two density matrices of rank $n-1$ in a Hilbert space of dimension $2n-2$. Indeed, the subspace $\mathcal{K}_{\rho'_0} \cap \mathcal{S}_{\rho'_1}$ is one dimensional and leads to the detection of ρ'_1 with unit probability. We call $|e'\rangle$ the unit vector spanning this 1-dimensional subspace. We are left with a reduce USD problem in a $2n-2$ dimensional Hilbert space. Importantly, $|e'\rangle$ is in $\mathcal{K}_{\rho'_0} \cap \mathcal{S}_{\rho'_1} \subset \mathcal{S}_{\rho'_0}^\perp = \mathcal{S}_{\rho_0}^\perp$. Indeed, $\mathcal{H} = \mathcal{S}_{\rho_0} \oplus \mathcal{S}_{\rho_0}^\perp = \mathcal{S}_{\rho'_0} \oplus \mathcal{S}_{|e\rangle} \oplus \mathcal{S}_{\rho_0}^\perp$ so that, in $\mathcal{H}' = \mathcal{H} / \mathcal{S}_{|e\rangle}$, $\mathcal{S}_{\rho'_0}^\perp = \mathcal{S}_{\rho_0}^\perp$.

In other words, if $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1$ are not positive then it exists $|e\rangle$ in \mathcal{S}_{P_0} , eigenvector of $E_?$ with eigenvalue 1 and $|e'\rangle$ in \mathcal{K}_{ρ_0} , eigenvector of E_1 with eigenvalue 1. Without the assumption that $\text{rk}(E_0) < \text{rk}(\rho_i)$, we have in general that if $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1$ are not positive then there exists $|e\rangle$ in either \mathcal{S}_{P_0} or \mathcal{S}_{P_1} , eigenvector of $E_?$ with eigenvalue 1 and $|e'\rangle$ in either \mathcal{K}_{ρ_0} eigenvector of E_1 with eigenvalue 1 or \mathcal{K}_{ρ_1} , eigenvector of E_0 with eigenvalue 1. The completes the proof. ■

The third consequence of Theorem 18 is the derivation of the optimal USD measurement for any pair of two geometrically uniform states in four dimensions.

5.4 Second class of exact solutions

Geometrically uniform states, or GU states, are a generalization of symmetric states [50, 51, 52, 22, 53, 36]. While symmetric state are generated from one generator state and a single unitary transformation, GU states are generated from one generator and a group of unitaries. They are interesting for both practical and theoretical considerations. On the practical side, real applications often exhibit strong symmetries like GU symmetry². On the theoretical side, this symmetry allows us to seek for simpler conditions and then new results. Actually Eldar proved that the optimal measurement to unambiguously discriminate *geometrically uniform* states can be chosen *geometrically uniform*, too. This result allows us to derive now the general solution for unambiguously discriminating any pair of GU states in four dimension. Next we give the mathematical definition of the *geometrically uniform* states before presenting the optimal failure probability for unambiguously discriminating two *geometrically uniform* states in four dimensions and the corresponding optimal measurement.

5.4.1 Geometrically uniform states

A set of GU state is a set of mixed states $\{\rho_i\}$, $i = 1, \dots, n$ such that $\rho_i = U_i \rho U_i^\dagger$ where ρ is an arbitrary density matrix called the *generator* and the set $\{U_i\}$, $i = 1, \dots, n$ is a set of unitary matrices that form an abelian group. In order not to break the symmetry of the states, we assume that all their *a priori* probabilities are equal to $\frac{1}{n}$.

A consequence of the group structure of the set $\{U_i\}$ is that we can always consider U_1 as the identity, and ρ_1 as the generator for a given set of GU states. We can therefore always write two GU states as ρ_0 and $\rho_1 = U \rho_0 U$ where U is an involution (i.e. a unitary transformation U such that $U^2 = \mathbb{1}$) with $\eta_0 = \eta_1 = \frac{1}{2}$. Let us note that two GU states are two symmetric states since only a single unitary is needed.

In the next section, we give a second class of exact solutions for USD of two generic density matrices. We provide the optimal failure probability as well as the optimal USD measurement for any two GU states in four dimensions.

²In a cryptographic context, the *bit value* states and *basis* states in the BB84-type protocol using weak coherent pulses and a phase reference exhibit such a GU symmetry.

5.4.2 Optimal unambiguous discrimination of two geometrically uniform states in four dimensions

Theorem 19 *Optimal unambiguous discrimination of two geometrically uniform states in four dimension*

Consider a USD problem defined by two geometrically uniform states ρ_0 and ρ_1 of rank two with equal a priori probabilities and spanning a four-dimensional Hilbert space. Let F_0 and F_1 be the two operators $\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. The fidelity F of the two states ρ_0 and ρ_1 is then given by $F = \text{Tr}(F_0) = \text{Tr}(F_1)$. We denote by P_0 and P_1 , the projectors onto the support of ρ_0 and ρ_1 . The optimal failure probability Q^{opt} for USD then satisfies

$$1. Q^{\text{opt}} = F \text{ if } \rho_0 - F_0 \geq 0 \quad (5.49)$$

$$2. Q^{\text{opt}} = 1 - \langle x | \rho_0 | x \rangle \text{ if } \begin{cases} \rho_0 - F_0 \not\geq 0 \\ \text{Spec}(P_1^\perp U P_1^\perp) = \{a, -b\}, a, b \in \mathbb{R}^+ \end{cases}$$

$$3. Q^{\text{opt}} = 1 \text{ otherwise.}$$

with $P_1^\perp U P_1^\perp = a|0\rangle\langle 0| - b|1\rangle\langle 1|$ and $|x\rangle = \frac{1}{\sqrt{a+b}}(e^{-i\text{Arg}(\langle 1|\rho_0|0\rangle)}\sqrt{b}|0\rangle + \sqrt{a}|1\rangle)$.

The POVM elements that realize these optimal failure probabilities are given in the different cases by

$$1. E_0 = \Sigma^{-1}\sqrt{\rho_0}(\rho_0 - F_0)\sqrt{\rho_0}\Sigma^{-1} \quad (5.50)$$

$$E_1 = U E_0 U$$

$$E_? = \mathbb{1} - E_0 - U E_0 U$$

$$2. E_0 = |x\rangle\langle x|$$

$$E_1 = U E_0 U$$

$$E_? = \mathbb{1} - E_0 - U E_0 U$$

$$3. E_0 = 0$$

$$E_1 = 0$$

$$E_? = \mathbb{1}.$$

Proof We consider a USD problem defined by two *geometrically uniform* states ρ_0 and $\rho_1 = U\rho_0U$, $U^2 = \mathbb{1}$, of rank two, spanning a four-dimensional Hilbert space. This means in

particular that $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ and $r_{E_0}^{\max} = r_{E_1}^{\max} = r_{E_?}^{\max} = 2$.

Due to the symmetry of the states, we also notice that $\rho_0 - F_0 = \rho_1 - F_1$. Note that the *a priori* probabilities are equal in order not to break the symmetry. Moreover, thanks to Eldar [36], we can choose the optimal USD measurement to be GU, too. Thus the POVM elements are such that

$$\begin{aligned} E_0 & , \\ E_1 & = UE_0U, \\ E_? & = UE_?U. \end{aligned} \tag{5.51}$$

The statement in Theorem 16 for equal *a priori* probability

$$Q^{\text{opt}} = F \Leftrightarrow \begin{aligned} \rho_0 - F_0 & \geq 0 \\ \rho_1 - F_1 & \geq 0 \end{aligned} \tag{5.52}$$

then reduces to

$$Q^{\text{opt}} = F \Leftrightarrow \rho_0 - F_0 \geq 0. \tag{5.53}$$

Note that we are not interested in the equivalence. The implication from the right to the left is the only important direction for our purpose here. In that case we need the assumption $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ to prove that: If $\rho_0 - F_0 \geq 0$ then $Q^{\text{opt}} = F$. Without this assumption, only the other direction is true.

If $\rho_0 - F_0 \not\geq 0$, Theorem 18 tells us that the ranks of the POVM elements E_0 and E_1 are not maximum (E_0 and E_1 have the same rank because of the symmetry). As a consequence, if $\rho_0 - F_0 \not\geq 0$ then $\text{rank}(E_0) = \text{rank}(E_1) < 2$. It follows that if $\rho_0 - F_0 \not\geq 0$ then the two POVM elements E_0 and E_1 have either rank 1 or rank 0. If $\text{rank}(E_0) = \text{rank}(E_1) = 0$ then $E_? = \mathbb{1}$ and $Q = 1$. Let us now focus on the remaining case $\text{rank}(E_0) = \text{rank}(E_1) = 1$.

Let us now prove that a measurement with $\text{rank}(E_0) = \text{rank}(E_1) = 1$ and $\text{rank}(E_?) \leq 2$ is necessary a projective measurement with $\text{rank}(E_?) = 2$. We can introduce the unit vectors and real numbers $|x\rangle \in \mathcal{K}_{\rho_1}$, $|y\rangle \in \mathcal{K}_{\rho_0}$, x and y such that

$$E_0 = x|x\rangle\langle x|, E_1 = y|y\rangle\langle y|. \tag{5.54}$$

We call \mathcal{S}_{xy} the two dimensional subspace spanned by $|x\rangle$ and $|y\rangle$, P_{xy} the projection onto it and P_{xy}^\perp the projector onto its orthogonal complement. By definition of the subspace \mathcal{S}_{xy} ,

$$P_{xy}^\perp E_? P_{xy}^\perp = P_{xy}^\perp. \tag{5.55}$$

Therefore $\text{rank}(P_{xy}^\perp E_\gamma P_{xy}^\perp) = \text{rank}(P_{xy}^\perp) = 2$ and E_γ must be at least of rank 2. However $\text{rank}(E_\gamma) \leq 2$. Therefore $\text{rank}(E_\gamma) = 2$ and

$$E_\gamma = P_{xy}^\perp. \quad (5.56)$$

We can now consider the subspace \mathcal{S}_{xy} only. On that subspace, we have

$$E_0 + E_1 = P_{\mathcal{S}_{xy}} \quad (5.57)$$

that is to say $P_{xy} = x|x\rangle\langle x| + y|y\rangle\langle y|$. Since P_{xy} is a projector, $P_{xy} = P_{xy}^2$ and it follows that $x|x\rangle\langle x| + y|y\rangle\langle y| + xy\langle y|x\rangle|y\rangle\langle x| + xy\langle y|x\rangle|y\rangle\langle x| = x|x\rangle\langle x| + y|y\rangle\langle y|$. The off-diagonal terms are equal if and only if $\langle y|x\rangle = 0$ while the diagonal terms are equal if and only if $x = y = 1$. The POVM then is a projective measurement with $\text{rank}(E_\gamma) = 2$.

We now give the optimal USD measurement for a GU projective measurement. Since the measurement is made of projectors, we have $\text{Tr}(E_0 E_1) = 0$ which is nothing but $\langle x|U|x\rangle = 0$. Because $|x\rangle$ lies in \mathcal{K}_{ρ_1} , this relation is equivalent to

$$\langle x|P_1^\perp U P_1^\perp|x\rangle = 0. \quad (5.58)$$

$P_1^\perp U P_1^\perp$ is a Hermitian operator and therefore owns real eigenvalues. Note that if $P_1^\perp U P_1^\perp$ must be of rank 2 since U is full rank. Thus we denote a and c the two eigenvalues of $P_1^\perp U P_1^\perp$ and $|0\rangle$ and $|1\rangle$ its two eigenvectors. In this eigenbasis, $|x\rangle \in \mathcal{K}_{\rho_1}$ can be expressed as

$$|x\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad (5.59)$$

This leads to $\langle x|P_1^\perp U P_1^\perp|x\rangle = |\alpha|^2 a + |\beta|^2 c$. Importantly this scalar product can only vanish if $a > 0$ and $c < 0$. We call $-c = b > 0$ such that, in $\{|0\rangle, |1\rangle\}$,

$$P_1^\perp U P_1^\perp = \begin{pmatrix} a & 0 \\ 0 & -b \end{pmatrix}. \quad (5.60)$$

If we include the normalization of $|x\rangle$, we end up with a system of two equations. This system simply is

$$\begin{cases} |\alpha|^2 a + |\beta|^2 c = 0 \\ |\alpha|^2 + |\beta|^2 = 1 \end{cases} \quad (5.61)$$

and admits a family of solutions parametrized by a phase Φ :

$$\{\alpha = \frac{e^{i\Phi}}{\sqrt{1+a/b}}, \beta = \frac{1}{\sqrt{1+b/a}}\}. \quad (5.62)$$

In the basis $\{|0\rangle, |1\rangle\}$ we can therefore write

$$|x\rangle = \begin{pmatrix} \frac{e^{i\Phi}}{\sqrt{1+a/b}} \\ \frac{1}{\sqrt{1+b/a}} \end{pmatrix}. \quad (5.63)$$

We can use again the fact that we are interested in the optimal measurement. Note that we already considered optimality to state that if $\rho_0 - F_0 \not\geq 0$ then the POVM is either $\{E_0 = E_1 = 0, E_2 = \mathbb{1}\}$ or a projective measurement. Indeed Theorem 18 is only concerned with optimal USD POVM. So far, $|x\rangle$ is valid for any USD measurement such that $E_0 = |x\rangle\langle x|$, $E_1 = UE_0U$ and $E_2 = \mathbb{1} - E_0 - UE_0U$. Let us now find the optimal one. To do so, we evaluate the success probability $P_{success}^{\text{opt}}$. Because of the symmetry of the two GU states, $\text{Tr}(E_0\rho_0) = \text{Tr}(E_1\rho_1)$ and the success probability $P_{success}^{\text{opt}} = \frac{1}{2}\text{Tr}(E_0\rho_0) + \frac{1}{2}\text{Tr}(E_1\rho_1)$ for unambiguously discriminating the two GU state ρ_0 and ρ_1 takes the form

$$P_{success}^{\text{opt}} = \text{Tr}(E_0\rho_0) = \langle x|\rho_0|x\rangle. \quad (5.64)$$

After calculation, we obtain

$$P_{success}^{\text{opt}} = \frac{1}{a+b} \left(b\langle 0|\rho_0|0\rangle + a\langle 1|\rho_0|1\rangle + 2\sqrt{ab}\text{Re}(\langle 0|\rho_0|1\rangle e^{i\Phi}) \right). \quad (5.65)$$

We choose the phase Φ to maximize this success probability $P_{success}^{\text{opt}}$. That is why we choose Φ such that $\text{Re}(\langle 0|\rho_0|1\rangle e^{i\Phi}) = |\langle 0|\rho_0|1\rangle|$. Therefore, Φ must be $-\text{Arg}(\langle 0|\rho_0|1\rangle)$ and

$$|x\rangle = \begin{pmatrix} \frac{e^{-i\text{Arg}(\langle 0|\rho_0|1\rangle)}}{\sqrt{1+a/b}} \\ \frac{1}{\sqrt{1+b/a}} \end{pmatrix}. \quad (5.66)$$

This completes the proof. ■

This theorem leads to a fundamental question: 'Is it possible to find a unified expression for the failure probability Q ?' In the first class of exact solutions, we can write the three failure probabilities of the three regimes as

$$Q = \alpha\eta_0F + \frac{1}{\alpha}\eta_1F$$

with the above-mentioned α . But we do not really expect the bounds in the outer regimes to be often optimal (see discussion in section 5.2) so that this expression does not seem so fundamental. More significantly, for the second class of exact solutions, no unified expression of the failure probability exists. In higher dimension ($\dim(\mathcal{H}) > 4$), the number of cases for the optimal failure probability Q might become very large. If this is the case, a unified expression for Q would be a pre-condition to find the general solution to USD of two density matrices.

In the next chapter we analyze an application of both theoretical and practical interest. In fact, we consider the *Bennett and Brassard 1984* protocol (BB84 protocol) implemented through weak coherent pulses with strong phase reference. This represents the first solved example of a non reducible USD problem.

Chapter 6

Application of the second class of exact solutions to the BB84 protocol

In 1984, Bennett and Brassard proposed a protocol to distribute a unconditional secure private key between two parties over a public channel in order to allow a secure communication. This proposed Quantum Key Distribution protocol, the so-called Bennett-Brassard 1984 (or shortly BB84) is here unconditional secure because of the laws of nature (quantum mechanics) and not anymore because of the assumption of a limited computational power of some hypothetical eavesdropper. In the standard BB84 protocol, Alice sends one of the four states $\{0, 1, +, -\}$ to Bob. Here $\{0, 1\}$ and $\{+, -\}$ are orthogonal pairs and 0 and $+$ correspond to the *bit value* 0 while 1 and $-$ correspond to the *bit value* 1. Bob then detects the signal sent in one of the two bases $\{0, 1\}$ or $\{+, -\}$.

In this thesis, we consider the implementation of a BB84-type protocol that uses weak coherent pulses with a phase reference. In that scenario, Alice sends one of the four states $\{|\frac{\alpha}{\sqrt{2}}\rangle|\frac{\pm\alpha}{\sqrt{2}}\rangle, |\frac{\alpha}{\sqrt{2}}\rangle|\frac{\pm i\alpha}{\sqrt{2}}\rangle\}$. The *bit value* is encoded in the sign of the coherent states that is to say $|\frac{\alpha}{\sqrt{2}}\rangle$ and $|\frac{i\alpha}{\sqrt{2}}\rangle$ correspond to the *bit value* 0, $|\frac{-\alpha}{\sqrt{2}}\rangle$ and $|\frac{-i\alpha}{\sqrt{2}}\rangle$ correspond to the *bit value* 1. Moreover the phase i plays the role of the basis in the standard BB84 protocol. Firstly let us note that the factor $\frac{1}{\sqrt{2}}$ in the amplitude comes from the technique used to implement the polarized coherent states. Secondly the first mode $|\frac{\alpha}{\sqrt{2}}\rangle$ is common to the four signal states. This mode is therefore irrelevant for the following analyze. Furthermore it is worth noticing that the states corresponding to the *bit value* 0 and 1 are not orthogonal since

$$\langle \frac{\alpha}{\sqrt{2}} | \frac{-\alpha}{\sqrt{2}} \rangle \neq 0, \quad (6.1)$$

$$\langle \frac{i\alpha}{\sqrt{2}} | \frac{-i\alpha}{\sqrt{2}} \rangle \neq 0. \quad (6.2)$$

This QKD protocol is therefore not the standard BB84 protocol. It remains that two important question can be addressed.

With what probability can an eavesdropper unambiguously distinguish the *basis* of the signal?

With what probability can an eavesdropper unambiguously determine which *bit value* is sent without being interested in the knowledge of the basis?

In fact the first question refers to the unambiguous discrimination of the two *basis* $\{|\frac{\pm\alpha}{\sqrt{2}}\rangle\}$ and $\{|\frac{\pm i\alpha}{\sqrt{2}}\rangle\}$. Therefore we can build a mixed state ρ_0 that corresponds to the basis $\{|\frac{\pm\alpha}{\sqrt{2}}\rangle\}$ and a mixed state ρ_1 for the basis $\{|\frac{\pm i\alpha}{\sqrt{2}}\rangle\}$. We end up with

$$\rho_0 = \frac{1}{2} \left(\left| \frac{\alpha}{\sqrt{2}} \right\rangle \left\langle \frac{\alpha}{\sqrt{2}} \right| + \left| \frac{-\alpha}{\sqrt{2}} \right\rangle \left\langle \frac{-\alpha}{\sqrt{2}} \right| \right), \quad (6.3)$$

$$\rho_1 = \frac{1}{2} \left(\left| \frac{i\alpha}{\sqrt{2}} \right\rangle \left\langle \frac{i\alpha}{\sqrt{2}} \right| + \left| \frac{-i\alpha}{\sqrt{2}} \right\rangle \left\langle \frac{-i\alpha}{\sqrt{2}} \right| \right). \quad (6.4)$$

where we ignore the irrelevant first mode.

The second question refers to the unambiguous discrimination of the two *bit value* mixed states. We can for that case build the two density matrices

$$\rho_0 = \frac{1}{2} \left(\left| \frac{\alpha}{\sqrt{2}} \right\rangle \left\langle \frac{\alpha}{\sqrt{2}} \right| + \left| \frac{i\alpha}{\sqrt{2}} \right\rangle \left\langle \frac{i\alpha}{\sqrt{2}} \right| \right), \quad (6.5)$$

$$\rho_1 = \frac{1}{2} \left(\left| \frac{-\alpha}{\sqrt{2}} \right\rangle \left\langle \frac{-\alpha}{\sqrt{2}} \right| + \left| \frac{-i\alpha}{\sqrt{2}} \right\rangle \left\langle \frac{-i\alpha}{\sqrt{2}} \right| \right) \quad (6.6)$$

where we again ignore the irrelevant first mode.

The states $\{|\frac{\pm\alpha}{\sqrt{2}}\rangle\}, \{|\frac{\pm i\alpha}{\sqrt{2}}\rangle\}$ are four linearly independent pure states. Therefore they span a four dimension Hilbert space. In the next section we will express the four density matrices above in that four dimensional Hilbert space and prove that they are GU states. After that, we will solve the two USD problems arising from the two questions mentioned. It turns out that the first case is reducible to some pure state case while the second one requires our last theorem to be solved. Let us now start with the explicit expression of these four mixed states.

6.1 Two geometrically uniform states in a four-dimensional Hilbert space

A coherent state of amplitude α can be written as a poisson distribution of photon number in the polarization mode a^\dagger as

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{(\alpha a^\dagger)^n}{n!} |0\rangle, \quad (6.7)$$

where $|0\rangle$ denotes the vacuum state. Moreover, the four signal states $|\pm\alpha\rangle, |i\pm\alpha\rangle$ are coherent states in four different polarizations: $\pm 45^\circ$ and circular left or right. These polarizations are expressed in terms of two orthogonal polarizations b_1^\dagger and b_2^\dagger as

$$a_0^\dagger = \frac{1}{\sqrt{2}}(b_1^\dagger + b_2^\dagger), \quad (6.8)$$

$$a_1^\dagger = \frac{1}{\sqrt{2}}(b_1^\dagger + ib_2^\dagger), \quad (6.9)$$

$$a_2^\dagger = \frac{1}{\sqrt{2}}(b_1^\dagger - b_2^\dagger), \quad (6.10)$$

$$a_3^\dagger = \frac{1}{\sqrt{2}}(b_1^\dagger - ib_2^\dagger). \quad (6.11)$$

Consequently, we can write the four states as

$$|\Psi_0\rangle = \left|\frac{\alpha}{\sqrt{2}}\right\rangle \left|\frac{\alpha}{\sqrt{2}}\right\rangle, \quad (6.12)$$

$$|\Psi_1\rangle = \left|\frac{\alpha}{\sqrt{2}}\right\rangle \left|\frac{i\alpha}{\sqrt{2}}\right\rangle, \quad (6.13)$$

$$|\Psi_2\rangle = \left|\frac{\alpha}{\sqrt{2}}\right\rangle \left|\frac{-\alpha}{\sqrt{2}}\right\rangle, \quad (6.14)$$

$$|\Psi_3\rangle = \left|\frac{\alpha}{\sqrt{2}}\right\rangle \left|\frac{-i\alpha}{\sqrt{2}}\right\rangle. \quad (6.15)$$

The first mode is common to the four states and therefore will be left out. In the phase space, these four states are generated from $|\Psi_0\rangle$ and a rotation of angle $\frac{\pi}{2}$. This means they are symmetric states and we can write them in a suitable basis following Chefles *et al.* [19]. The idea is that n symmetric states can always be written in an orthonormal basis $\{|\Phi_j\rangle\}$ as

$$|\Psi_k\rangle = \sum_{j=0}^{n-1} c_j e^{2i\pi \frac{kj}{n}} |\Phi_j\rangle. \quad (6.16)$$

Note that the phase of the complex numbers c_j is not relevant since we can absorb it in the definition of the basis elements $|\Phi_j\rangle$. Actually the modulus of the coefficients c_j s can be expressed

[19] as

$$|c_j|^2 = \frac{1}{n^2} \sum_{k,k'} e^{-2i\pi \frac{j(k-k')}{n}} \langle \Psi'_k | \Psi_k \rangle. \quad (6.17)$$

This leads in our case to

$$|c_0| = \frac{1}{\sqrt{2}} e^{-\frac{\mu}{4}} \sqrt{\cosh\left(\frac{\mu}{2}\right) + \cos\left(\frac{\mu}{2}\right)}, \quad (6.18)$$

$$|c_1| = \frac{1}{\sqrt{2}} e^{-\frac{\mu}{4}} \sqrt{\sinh\left(\frac{\mu}{2}\right) + \sin\left(\frac{\mu}{2}\right)}, \quad (6.19)$$

$$|c_2| = \frac{1}{\sqrt{2}} e^{-\frac{\mu}{4}} \sqrt{\cosh\left(\frac{\mu}{2}\right) - \cos\left(\frac{\mu}{2}\right)}, \quad (6.20)$$

$$|c_3| = \frac{1}{\sqrt{2}} e^{-\frac{\mu}{4}} \sqrt{\sinh\left(\frac{\mu}{2}\right) - \sin\left(\frac{\mu}{2}\right)}. \quad (6.21)$$

where $\mu = |\alpha|^2$ stands for the mean photon number. Moreover, in the basis $\{|\Phi_j\rangle\}$, the unitary transformation acting on $|\Psi_0\rangle$ that generates the other three states is

$$K = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix} \quad (6.22)$$

such that $K^4 = \mathbb{1}$. The four symmetric states (see Fig. 6.1) are then expressed as

$$|\Psi_0\rangle = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix}, \quad (6.23)$$

$$|\Psi_1\rangle = K|\Psi_0\rangle = \begin{pmatrix} c_0 \\ ic_1 \\ -c_2 \\ -ic_3 \end{pmatrix}, \quad (6.24)$$

$$|\Psi_2\rangle = K^2|\Psi_0\rangle = \begin{pmatrix} c_0 \\ -c_1 \\ c_2 \\ -c_3 \end{pmatrix}, \quad (6.25)$$

$$|\Psi_3\rangle = K^3|\Psi_0\rangle = \begin{pmatrix} c_0 \\ -ic_1 \\ -c_2 \\ ic_3 \end{pmatrix}. \quad (6.26)$$

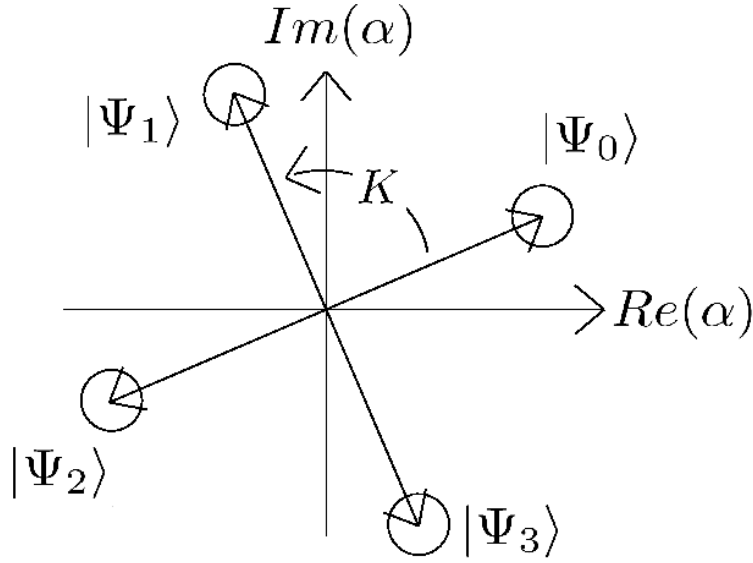


Figure 6.1: Schematic view of the four symmetric states in the phase space

At that point, we are ready to write the four density matrices corresponding to the *basis* mixed states and the *bit value* mixed states.

The *basis* mixed states (see Fig. 6.2)

$$\rho_0 = \frac{1}{2}(|\Psi_0\rangle\langle\Psi_0| + |\Psi_2\rangle\langle\Psi_2|), \quad (6.27)$$

$$\rho_1 = \frac{1}{2}(|\Psi_1\rangle\langle\Psi_1| + |\Psi_3\rangle\langle\Psi_3|) \quad (6.28)$$

are by construction of rank 2.

They can be written in a four dimensional Hilbert space spanned by the four linearly independent states $|\Psi_i\rangle$, $i = 0, 1, 2, 3$ as

$$\rho_0 = \begin{pmatrix} c_0^2 & 0 & c_0c_2 & 0 \\ 0 & c_1^2 & 0 & c_1c_3 \\ c_0c_2 & 0 & c_2^2 & 0 \\ 0 & c_1c_3 & 0 & c_3^2 \end{pmatrix} \quad (6.29)$$

and

$$\rho_1 = \begin{pmatrix} c_0^2 & 0 & -c_0c_2 & 0 \\ 0 & c_1^2 & 0 & -c_1c_3 \\ -c_0c_2 & 0 & c_2^2 & 0 \\ 0 & -c_1c_3 & 0 & c_3^2 \end{pmatrix} \quad (6.30)$$

where we choose all the coefficients c_i to be real.

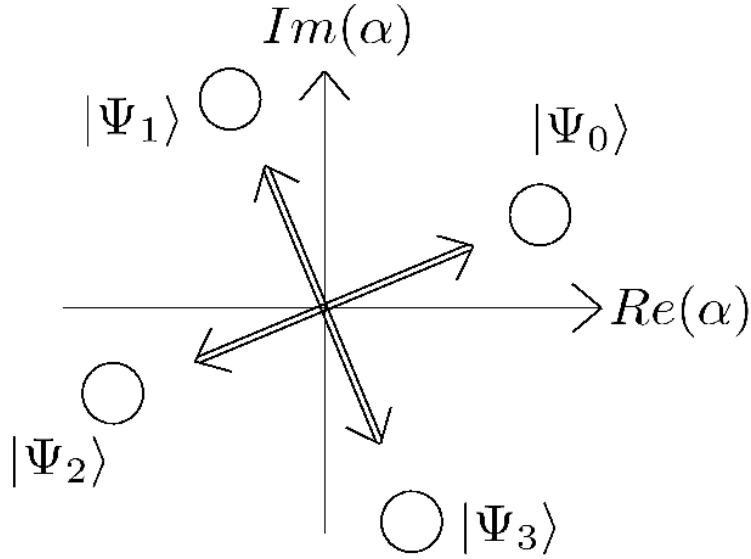


Figure 6.2: Pairing of the four symmetric states for the *basis* mixed states

Thanks to Eqn. (6.27) and Eqn. (6.28), we clearly see that

$$\rho_1 = K\rho_0K^\dagger = K^\dagger\rho_0K. \quad (6.31)$$

Moreover, we can calculate that $K\rho_0K = K^\dagger\rho_0K^\dagger$ in the following calculation.

$$K\rho_0K = \frac{1}{2}(K|\Psi_0\rangle\langle\Psi_0|K + K|\Psi_2\rangle\langle\Psi_2|K) \quad (6.32)$$

$$= \frac{1}{2}(|\Psi_1\rangle\langle\Psi_3| + |\Psi_3\rangle\langle\Psi_1|) \quad (6.33)$$

$$= \frac{1}{2}(K^\dagger|\Psi_2\rangle\langle\Psi_2|K^\dagger + K^\dagger|\Psi_0\rangle\langle\Psi_0|K^\dagger) \quad (6.34)$$

$$= K^\dagger\rho_0K^\dagger. \quad (6.35)$$

The consequence is that we can construct two new unitary matrices which are involution¹ such that $\rho_1 = U_\pm\rho_0U_\pm$. This two involutions are given by

$$U_\pm = \frac{K + K^\dagger}{2} \pm i\frac{K - K^\dagger}{2} = U_\pm^\dagger. \quad (6.36)$$

$$(6.37)$$

We can choose to use in the following calculation

$$U = U_- = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \quad (6.38)$$

¹A unitary transformation U is called an involution if and only if $U^2 = \mathbb{I}$.

We have finally written the *basis* mixed states as ρ_0 and $\rho_1 = U\rho_0U$ where $U^2 = \mathbb{1}$. This means that the question 'With what probability can an eavesdropper unambiguously distinguish the *basis* of the signal?' is related to the unambiguous discrimination of two geometrically uniform mixed states in dimension four. The choice of such an involution matrix will simplify the next calculations. Finally, in the four dimensional Hilbert space, we see that

$$\rho_0 + \rho_1 = \begin{pmatrix} c_0^2 & 0 & 0 & 0 \\ 0 & c_1^2 & 0 & 0 \\ 0 & 0 & c_2^2 & 0 \\ 0 & 0 & 0 & c_3^2 \end{pmatrix} \quad (6.39)$$

such that $\text{rank}(\rho_0 + \rho_1) = 4 = \text{rank}(\rho_0) + \text{rank}(\rho_1)$. The two GU states ρ_0 and ρ_1 do not have overlapping supports and we can apply Theorem 19 about USD of such a pair of states. The *bit value* mixed states (see Fig. 6.3) are also rank two matrices by construction. They can be written as

$$\rho_0 = \frac{1}{2}(|\Psi_0\rangle\langle\Psi_0| + |\Psi_1\rangle\langle\Psi_1|), \quad (6.40)$$

$$\rho_1 = \frac{1}{2}(|\Psi_2\rangle\langle\Psi_2| + |\Psi_3\rangle\langle\Psi_3|). \quad (6.41)$$

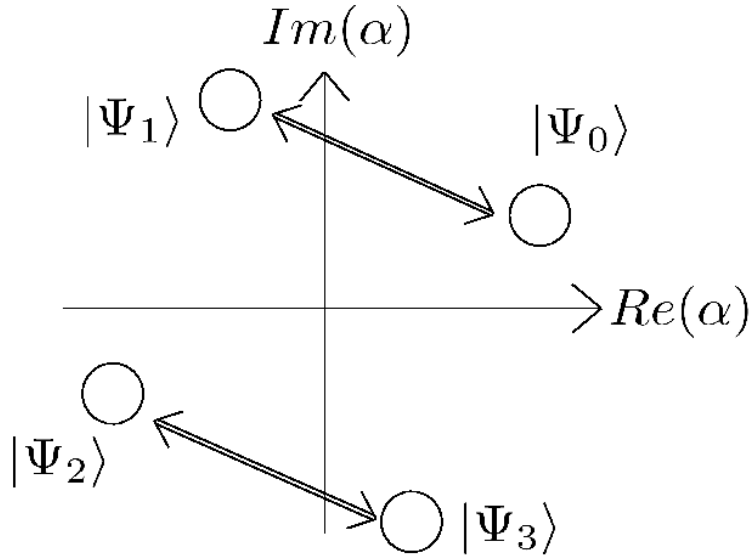


Figure 6.3: Pairing of the four symmetric states for the *bit value* mixed states

In terms of the coefficients c_i 's, we obtain the following form in the four dimensional Hilbert space spanned by the states $|\Psi_i\rangle$, $i = 0, 1, 2, 3$:

$$\rho_0 = \begin{pmatrix} c_0^2 & \frac{1-i}{2}c_0c_1 & 0 & \frac{1+i}{2}c_0c_3 \\ \frac{1+i}{2}c_1c_0 & c_1^2 & \frac{1-i}{2}c_1c_2 & 0 \\ 0 & \frac{1+i}{2}c_2c_1 & c_2^2 & \frac{1-i}{2}c_2c_3 \\ \frac{1-i}{2}c_3c_0 & 0 & \frac{1+i}{2}c_3c_2 & c_3^2 \end{pmatrix} \quad (6.42)$$

and

$$\rho_1 = \begin{pmatrix} c_0^2 & -\frac{1-i}{2}c_0c_1 & 0 & -\frac{1+i}{2}c_0c_3 \\ -\frac{1+i}{2}c_1c_0 & c_1^2 & -\frac{1-i}{2}c_1c_2 & 0 \\ 0 & -\frac{1+i}{2}c_2c_1 & c_2^2 & -\frac{1-i}{2}c_2c_3 \\ -\frac{1-i}{2}c_3c_0 & 0 & -\frac{1+i}{2}c_3c_2 & c_3^2 \end{pmatrix}. \quad (6.43)$$

It is unfortunately impossible to choose the phase of the coefficient c_i so that ρ_0 and ρ_1 are real matrices. Therefore we simply choose all the coefficient c_i to be real and we end up with

$$\rho_0 = \begin{pmatrix} c_0^2 & \frac{1-i}{2}c_0c_1 & 0 & \frac{1+i}{2}c_0c_3 \\ \frac{1+i}{2}c_1c_0 & c_1^2 & \frac{1-i}{2}c_1c_2 & 0 \\ 0 & \frac{1+i}{2}c_2c_1 & c_2^2 & \frac{1-i}{2}c_2c_3 \\ \frac{1-i}{2}c_3c_0 & 0 & \frac{1+i}{2}c_3c_2 & c_3^2 \end{pmatrix} \quad (6.44)$$

and

$$\rho_1 = \begin{pmatrix} c_0^2 & -\frac{1-i}{2}c_0c_1 & 0 & -\frac{1+i}{2}c_0c_3 \\ -\frac{1+i}{2}c_1c_0 & c_1^2 & -\frac{1-i}{2}c_1c_2 & 0 \\ 0 & -\frac{1+i}{2}c_2c_1 & c_2^2 & -\frac{1-i}{2}c_2c_3 \\ -\frac{1-i}{2}c_3c_0 & 0 & -\frac{1+i}{2}c_3c_2 & c_3^2 \end{pmatrix}. \quad (6.45)$$

The involution connected ρ_0 and ρ_1 simply is

$$K^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \quad (6.46)$$

Of course, the question 'With what probability can an eavesdropper unambiguously determine which *bit value* is sent without being interested in the knowledge of the basis?' is also related to the unambiguous discrimination of two geometrically uniform mixed states in dimension four. Here again, the sum $\rho_0 + \rho_1$ in the four dimensional Hilbert space is given by

$$\rho_0 + \rho_1 = \begin{pmatrix} c_0^2 & 0 & 0 & 0 \\ 0 & c_1^2 & 0 & 0 \\ 0 & 0 & c_2^2 & 0 \\ 0 & 0 & 0 & c_3^2 \end{pmatrix} \quad (6.47)$$

implying that the two GU states ρ_0 and ρ_1 do not have overlapping supports. Consequently Theorem 19 can be used.

Actually one could consider a third USD problem coming from the pairing of the four states Ψ_i (see Fig. 6.4). This last case is concerned with the unambiguous discrimination of the two mixed states $\rho_0 = \frac{1}{2}(|\Psi_0\rangle\langle\Psi_0| + |\Psi_3\rangle\langle\Psi_3|)$ and $\rho_1 = \frac{1}{2}(|\Psi_1\rangle\langle\Psi_1| + |\Psi_2\rangle\langle\Psi_2|)$ but this case is similar² to the previous case. Indeed one can go from the former to the later case by using the unitary K^2 . This is not the case between the two problems of unambiguously discriminating the *basis* states and the *bit value* states.

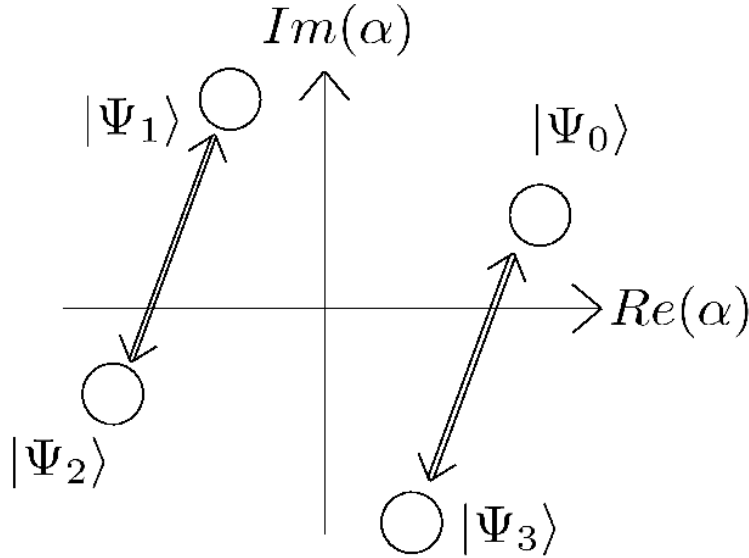


Figure 6.4: Third possible pairing of the four symmetric states

6.2 USD of the *basis* mixed states

Let us repeat that the two density matrices to unambiguously discriminate are

$$\rho_0 = \begin{pmatrix} c_0^2 & 0 & c_0 c_2 & 0 \\ 0 & c_1^2 & 0 & c_1 c_3 \\ c_0 c_2 & 0 & c_2^2 & 0 \\ 0 & c_1 c_3 & 0 & c_3^2 \end{pmatrix} \quad (6.48)$$

²unitary equivalent

and

$$\rho_1 = U\rho_0U = \begin{pmatrix} c_0^2 & 0 & -c_0c_2 & 0 \\ 0 & c_1^2 & 0 & -c_1c_3 \\ -c_0c_2 & 0 & c_2^2 & 0 \\ 0 & -c_1c_3 & 0 & c_3^2 \end{pmatrix}. \quad (6.49)$$

with

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \quad (6.50)$$

With a bit of concentration, one can realize that these two density matrices are block diagonal. Indeed, we can use the permutation matrix

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (6.51)$$

and obtain

$$P\rho_{0,1}P = \begin{pmatrix} c_0^2 & \pm c_0c_2 & 0 & 0 \\ \pm c_0c_2 & c_2^2 & 0 & 0 \\ 0 & 0 & c_1^2 & \pm c_1c_3 \\ 0 & 0 & \pm c_1c_3 & c_3^2 \end{pmatrix}. \quad (6.52)$$

This already tells us that we can analytically solve this problem which is reducible to some pure states case. Indeed ρ_0 and ρ_1 are block diagonal where each block is two dimensional. We will nevertheless use the non reduced density matrices to find the optimal USD measurement. The reason is that, as we will in the next paragraph, we can compute the operator $\rho_0 - F_0$ and check its positivity for any value of the amplitude α . Note here that the spectra of $\rho_0 - F_0$ and $\rho_1 - F_1$ are identical since $\rho_1 - F_1 = \rho_0 - F_0$ for two GU states. With that, we have the optimal failure probability as soon as the optimal measurement. Again, we could use the second and third reduction theorems but the present example gives us the opportunity to use other tools.

We now focus our attention onto ρ_0 only since ρ_1 is similar to it. The density matrix

$$P\rho_0P = \begin{pmatrix} c_0^2 & c_0c_2 & 0 & 0 \\ c_0c_2 & c_2^2 & 0 & 0 \\ 0 & 0 & c_1^2 & c_1c_3 \\ 0 & 0 & c_1c_3 & c_3^2 \end{pmatrix} \quad (6.53)$$

can be easily diagonalized using the block diagonal unitary matrices

$$PU_0P = \begin{pmatrix} \frac{c_0}{\sqrt{c_0^2 + c_2^2}} & \frac{c_2}{\sqrt{c_0^2 + c_2^2}} & 0 & 0 \\ \frac{c_2}{\sqrt{c_0^2 + c_2^2}} & \frac{-c_0}{\sqrt{c_0^2 + c_2^2}} & 0 & 0 \\ 0 & 0 & \frac{c_1}{\sqrt{c_1^2 + c_3^2}} & \frac{c_3}{\sqrt{c_1^2 + c_3^2}} \\ 0 & 0 & \frac{c_3}{\sqrt{c_1^2 + c_3^2}} & \frac{-c_1}{\sqrt{c_1^2 + c_3^2}} \end{pmatrix}. \quad (6.54)$$

If is not too difficult to find that the eigenvalues of $P\rho_0P$ are therefore given by

$$\lambda_0 = c_0^2 + c_2^2 \quad (6.55)$$

$$\lambda_1 = c_1^2 + c_3^2 \quad (6.56)$$

which gives, in terms of the mean photon number μ

$$\lambda_{0,1} = \frac{1 \pm e^{-\mu}}{2}. \quad (6.57)$$

If we undo everywhere the permutation matrix P , the density matrices $\rho_{0,1}$ can obviously be diagonalized with the help of the unitary transformation

$$U_0 = \begin{pmatrix} \frac{c_0}{\sqrt{c_0^2 + c_2^2}} & 0 & \frac{c_2}{\sqrt{c_0^2 + c_2^2}} & 0 \\ 0 & \frac{c_1}{\sqrt{c_1^2 + c_3^2}} & 0 & \frac{c_3}{\sqrt{c_1^2 + c_3^2}} \\ \frac{c_2}{\sqrt{c_0^2 + c_2^2}} & 0 & \frac{-c_0}{\sqrt{c_0^2 + c_2^2}} & 0 \\ 0 & \frac{c_3}{\sqrt{c_1^2 + c_3^2}} & 0 & \frac{-c_1}{\sqrt{c_1^2 + c_3^2}} \end{pmatrix}. \quad (6.58)$$

and its square root takes the form

$$\sqrt{\rho_0} = \begin{pmatrix} \frac{c_0^2}{\sqrt{c_0^2 + c_2^2}} & 0 & \frac{c_0 c_2}{\sqrt{c_0^2 + c_2^2}} & 0 \\ 0 & \frac{c_1^2}{\sqrt{c_1^2 + c_3^2}} & 0 & \frac{c_1 c_3}{\sqrt{c_1^2 + c_3^2}} \\ \frac{c_0 c_2}{\sqrt{c_0^2 + c_2^2}} & 0 & \frac{c_2^2}{\sqrt{c_0^2 + c_2^2}} & 0 \\ 0 & \frac{c_1 c_3}{\sqrt{c_1^2 + c_3^2}} & 0 & \frac{c_3^2}{\sqrt{c_1^2 + c_3^2}} \end{pmatrix}. \quad (6.59)$$

The next step is to calculate the operator $F_0 = \sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$. Our two GU states are related through the relation $\sqrt{\rho_1} = U\sqrt{\rho_0}U$. As a result, the equality $\sqrt{\rho_0}\sqrt{\rho_1} = F_0V$ leads to

$$\sqrt{\rho_0}U\sqrt{\rho_0} = F_0VU. \quad (6.60)$$

In the ρ_0 's eigenbasis, we obtain

$$U_0\sqrt{\rho_0}U\sqrt{\rho_0}U_0 = U_0F_0VUU_0 = U_0F_0U_0T \quad (6.61)$$

where $T = U_0 V U U_0$ is a unitary transformation. One can calculate the operator $U_0 \sqrt{\rho_0} U \sqrt{\rho_0} U_0$ and find

$$\begin{pmatrix} c_0^2 - c_2^2 & 0 & 0 & 0 \\ 0 & c_1^2 - c_3^2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (6.62)$$

which is always positive if multiplied by some signature matrix

$$T = \begin{pmatrix} \pm 1 & 0 & 0 & 0 \\ 0 & \pm 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (6.63)$$

Note here that, in terms of the mean photon number μ , the quantities $c_0^2 - c_2^2 = e^{\frac{-\mu}{2}} \cos \frac{\mu}{2}$ and $c_1^2 - c_3^2 = e^{\frac{-\mu}{2}} \sin \frac{\mu}{2}$ are not always positive. In the end, the positive operator F_0 is of the form

$$U_0 F U_0 = \begin{pmatrix} |c_0^2 - c_2^2| & 0 & 0 & 0 \\ 0 & |c_1^2 - c_3^2| & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (6.64)$$

The explicit form of the unitary V is only relevant to calculate the elements of the optUSDM. But our first goal is to find the spectrum of the operator $\rho_0 - F_0$. For that, four cases are to take into account depending on the sign of $c_0^2 - c_2^2$ and $c_1^2 - c_3^2$.

Everything is gathered to obtain the explicit form the operator $\rho_0 - F_0$ in the eigenbasis of ρ_0 . Indeed, we have

$$U_0(\rho_0 - F_0)U_0 = \begin{pmatrix} c_0^2 + c_2^2 & 0 & 0 & 0 \\ 0 & c_1^2 + c_3^2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} |c_0^2 - c_2^2| & 0 & 0 & 0 \\ 0 & |c_1^2 - c_3^2| & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (6.65)$$

$$= 2 \begin{pmatrix} \max\{c_0^2, c_2^2\} & 0 & 0 & 0 \\ 0 & \max\{c_1^2, c_3^2\} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \geq 0. \quad (6.66)$$

The spectrum of the operator $\rho_0 - F_0$ is positive for any value of the mean photon number μ . As a consequence, the optimal failure probability Q reaches the lower bounds $F = \text{Tr}(F_0) =$

$|c_0^2 - c_2^2| + |c_1^2 - c_3^2|$. In terms of the mean photon number μ (see Fig. 6.5), the optimal failure probability is given by

$$Q = e^{-\frac{\mu}{2}} \left(\left| \cos \frac{\mu}{2} \right| + \left| \sin \frac{\mu}{2} \right| \right). \quad (6.67)$$

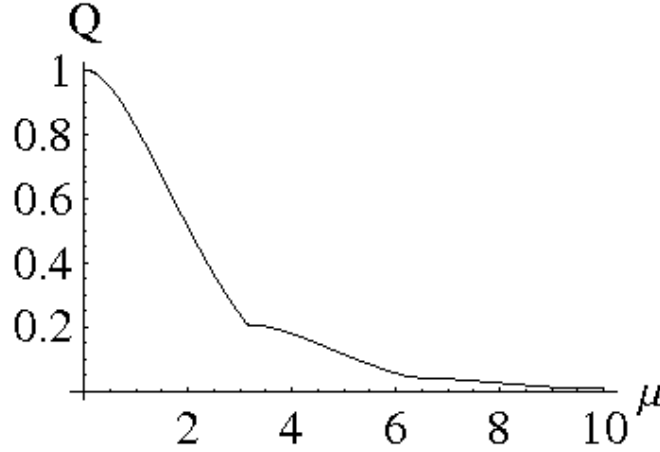


Figure 6.5: Optimal failure probability for USD of the *basis* mixed states

Let us note here that if we were interested in the unambiguous discrimination of

$$\rho_0 = \frac{1}{2} (|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|) \quad (6.68)$$

$$\text{and } \rho_1 = \frac{1}{2} (|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle -i\alpha|). \quad (6.69)$$

then we would find

$$Q = e^{-\mu} (|\cos\mu| + |\sin\mu|). \quad (6.70)$$

Let us conclude this section and this example by adding that we can give the optimal measurement to achieve $Q = F$. Indeed, the useful matrix Σ is diagonal and therefore its inverse simply is

$$\Sigma^{-1} = \begin{pmatrix} c_0^{-2} & 0 & 0 & 0 \\ 0 & c_1^{-2} & 0 & 0 \\ 0 & 0 & c_2^{-2} & 0 \\ 0 & 0 & 0 & c_3^{-2} \end{pmatrix}. \quad (6.71)$$

In the four different cases parametrized by the signature T , the elements of the optimal POVM are finally given by

$$E_0 = \Sigma^{-1} \sqrt{\rho_0} (\rho_0 - F_0) \sqrt{\rho_0} \Sigma^{-1} \quad (6.72)$$

$$E_1 = U E_0 U \quad (6.73)$$

$$E_? = \Sigma^{-1} (\sqrt{\rho_0} + \sqrt{\rho_1} V^\dagger) F_0 (\sqrt{\rho_0} + V \sqrt{\rho_1}) \Sigma^{-1} \quad (6.74)$$

where all the different matrices involved in these equations are perfectly known. This concludes this section and the first example.

6.3 USD of the *bit value* mixed states

The second case corresponds to the unambiguous discrimination of the two density matrices

$$\rho_0 = \begin{pmatrix} c_0^2 & \frac{1-i}{2}c_0c_1 & 0 & \frac{1+i}{2}c_0c_3 \\ \frac{1+i}{2}c_1c_0 & c_1^2 & \frac{1-i}{2}c_1c_2 & 0 \\ 0 & \frac{1+i}{2}c_2c_1 & c_2^2 & \frac{1-i}{2}c_2c_3 \\ \frac{1-i}{2}c_3c_0 & 0 & \frac{1+i}{2}c_3c_2 & c_3^2 \end{pmatrix} \quad (6.75)$$

and

$$\rho_1 = U\rho_0U = \begin{pmatrix} c_0^2 & -\frac{1-i}{2}c_0c_1 & 0 & -\frac{1+i}{2}c_0c_3 \\ -\frac{1+i}{2}c_1c_0 & c_1^2 & -\frac{1-i}{2}c_1c_2 & 0 \\ 0 & -\frac{1+i}{2}c_2c_1 & c_2^2 & -\frac{1-i}{2}c_2c_3 \\ -\frac{1-i}{2}c_3c_0 & 0 & -\frac{1+i}{2}c_3c_2 & c_3^2 \end{pmatrix} \quad (6.76)$$

with

$$U = K^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \quad (6.77)$$

This USD task is far more complicated than the first one. It is difficult to find the unitary transformations to diagonalize ρ_0 and ρ_1 and therefore the square root of those states as well as F_0 and F_1 cannot be easily expressed. We have to resort to a particular decomposition of the two states ρ_0 and ρ_1 . This decomposition allows us to diagonalize the operator $\rho_0 - F_0$ in an unknown basis and find its spectrum. First we review some relevant properties of the density matrices ρ_0 and ρ_1 . Next, we solve the unambiguous discrimination of these two GU states.

Actually one can write

$$\rho_0 = APA \quad (6.78)$$

where A is a real diagonal matrix and $P = \frac{p^2}{2}$ a pseudo projector. They are defined as

$$A = \begin{pmatrix} c_0 & 0 & 0 & 0 \\ 0 & c_1 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & 0 & c_3 \end{pmatrix} \quad (6.79)$$

and

$$P = \begin{pmatrix} 1 & \frac{1-i}{2} & 0 & \frac{1+i}{2} \\ \frac{1+i}{2} & 1 & \frac{1-i}{2} & 0 \\ 0 & \frac{1+i}{2} & 1 & \frac{1-i}{2} \\ \frac{1-i}{2} & 0 & \frac{1+i}{2} & 1 \end{pmatrix}. \quad (6.80)$$

Here come three remarks arising from this decomposition. First of all, let us note that they commute since they are both diagonal. Due to the symmetry between ρ_0 and ρ_1 and to the commutation between A and U , we have $\rho_1 = UAPAU = AUPUA$. Second of all, we can consider the sum of the two density matrices ρ_0 and ρ_1 . We have $\rho_0 + \rho_1 = APA + AUPUA = A(P + UPU)A$ and $P + UPU = 2\mathbb{1}$. Thus

$$\rho_0 + \rho_1 = 2A^2 \quad (6.81)$$

and we could denote $A = \sqrt{\frac{\Sigma}{2}}$. The last remark is the more important. Actually $\text{Tr}(P) = 4$. This is not a lot but it implies that P is equal to twice a two-dimensional projector. As a matter of fact, there exists a unitary transformation W so that

$$WPW^\dagger = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \quad (6.82)$$

Such a unitary matrix can be given by the Discrete Fourier Transform

$$W = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \quad (6.83)$$

The interest of the decomposition provide in Eqn.(6.78) is that it allows us to write $\rho_0 = APA$ in an unknown basis better suited to investigate the spectrum of the operator $\rho_0 - F_0$. Indeed we can write

$$\rho_0 = APA \quad (6.84)$$

$$= \frac{AP}{\sqrt{2}} \frac{PA}{\sqrt{2}} \quad (6.85)$$

$$= \sqrt{\rho_0} R_0^\dagger R_0 \sqrt{\rho_0} \quad (6.86)$$

where we introduce the unitary transformation R_0 such that $\frac{PA}{\sqrt{2}} = R_0 \sqrt{\rho_0}$. Consequently, we obtain

$$R_0 \rho_0 R_0^\dagger = \frac{PA}{\sqrt{2}} \frac{AP}{\sqrt{2}} \quad (6.87)$$

$$= \frac{PA^2 P}{2} \quad (6.88)$$

For the unambiguous discrimination of the two *basis* mixed states, we knew the unitary transformation U_0 that diagonalizes ρ_0 . It was possible to write F_0 and finally express the operator $\rho_0 - F_0$. Here we can not directly work with the eigenbasis of ρ_0 . Instead, we try to use the matrix $R_0\rho_0R_0^\dagger$, knowing only the existence of this unitary transformation R_0 . We are only interested in the spectrum of $\rho_0 - F_0$ and the precise form of R_0 is finally irrelevant as long as it permits us to find the spectrum of $\rho_0 - F_0$. Nevertheless, we must say, that the explicit expression of the POVM elements will not be provided since, in that case, we do need to know R_0 . Moreover, as we will soon see, we will not be able to calculate the complete expression of Q for all the regime of the mean photon number μ .

Let us now calculate the spectrum of $\rho_0 - F_0$. We first apply the Fourier Transform W onto $R_0\rho_0R_0^\dagger$ to end up with

$$WR_0\rho_0R_0^\dagger W^\dagger = \frac{1}{2}WPA^2PW^\dagger \quad (6.89)$$

$$= \frac{1}{2} \begin{pmatrix} c_0^2 + c_1^2 + c_2^2 + c_3^2 & 0 & 0 & c_0^2 + ic_1^2 - c_2^2 - ic_3^2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ c_0^2 - ic_1^2 - c_2^2 + ic_3^2 & 0 & 0 & c_0^2 + c_1^2 + c_2^2 + c_3^2 \end{pmatrix}. \quad (6.90)$$

Actually, since the states ρ_0 is normalized, we have $c_0^2 + c_1^2 + c_2^2 + c_3^2 = 1$ and therefore

$$WR_0\rho_0R_0^\dagger W^\dagger = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & \Lambda \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \Lambda^* & 0 & 0 & 1 \end{pmatrix}. \quad (6.91)$$

where

$$\Lambda = (c_0^2 - c_2^2) + i(c_1^2 - c_3^2). \quad (6.92)$$

In fact, a Hermitian matrix of the form

$$\begin{pmatrix} a & be^{i\phi} \\ be^{-i\phi} & a \end{pmatrix} \quad (6.93)$$

with a , b and ϕ real and positive, has for eigenvalues

$$\lambda_{\pm} = a \pm b \quad (6.94)$$

and for eigenvectors

$$|v_{\pm}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} \pm e^{i\phi} \\ 1 \end{pmatrix}. \quad (6.95)$$

Here we are only interested in the spectrum of ρ_0 . The formula above gives us its eigenvalues as

$$\lambda_{\pm} = \frac{1 \pm |\Lambda|}{2} \quad (6.96)$$

$$= \frac{1 \pm e^{-\frac{\mu}{2}}}{2}. \quad (6.97)$$

As for the *basis* mixed states case where we calculate the operator $U_0 \sqrt{\rho_0} U \sqrt{\rho_0} U_0$, we now consider the operator $WR_0 \sqrt{\rho_0} U \sqrt{\rho_0} R_0^\dagger W^\dagger$. Actually this operator is of a similar form than $WR_0 \rho_0 R_0^\dagger W^\dagger$. Indeed we obtain

$$WR_0 \sqrt{\rho_0} U \sqrt{\rho_0} R_0^\dagger W^\dagger = \frac{1}{2} \begin{pmatrix} (c_1^2 + c_3^2) - (c_0^2 + c_2^2) & 0 & 0 & -\Lambda^* \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -\Lambda & 0 & 0 & (c_1^2 + c_3^2) - (c_0^2 + c_2^2) \end{pmatrix}. \quad (6.98)$$

Thanks to Eqn.(6.94), we find that its eigenvalues are

$$\gamma_{\pm} = (c_1^2 + c_3^2) - (c_0^2 + c_2^2) \pm |\Lambda|. \quad (6.99)$$

Moreover, with the help of Eqn.(6.95), we obtain the unitary that diagonalizes the operator $WR_0 \sqrt{\rho_0} U \sqrt{\rho_0} R_0^\dagger W^\dagger$. This unitary is of form

$$K^\dagger = \frac{1}{\sqrt{2}} \begin{pmatrix} -\frac{\Lambda^*}{|\Lambda|} & 0 & 0 & \frac{\Lambda^*}{|\Lambda|} \\ 0 & \sqrt{2} & 0 & 0 \\ 0 & 0 & \sqrt{2} & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \quad (6.100)$$

If we replace the coefficients c_i by their expressions in term of the mean photon number μ , we end up with

$$KWR_0 \sqrt{\rho_0} U \sqrt{\rho_0} R_0^\dagger W^\dagger K^\dagger = \frac{1}{2} \begin{pmatrix} -e^{-\mu} + e^{-\frac{\mu}{2}} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -e^{-\mu} - e^{-\frac{\mu}{2}} \end{pmatrix}. \quad (6.101)$$

The eigenvalues in the top left corner is always positive while the eigenvalue in the bottom right corner is always negative. Therefore the operator F_0 in its eigenbasis is of the form

$$KWR_0 F_0 R_0 W^\dagger K^\dagger = KWR_0 \sqrt{\rho_0} U \sqrt{\rho_0} R_0^\dagger W^\dagger K^\dagger T \quad (6.102)$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} e^{-\frac{\mu}{2}} - e^{-\mu} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{-\frac{\mu}{2}} + e^{-\mu} \end{pmatrix} \quad (6.103)$$

and the unitary matrix V equals $R_0^\dagger W^\dagger K^\dagger T K W R_0 U$, where T is the signature

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \quad (6.104)$$

We have now all the necessary matrices to calculate the operator $\rho_0 - F_0$ in the F_0 's eigenbasis. We obtain

$$\begin{aligned} K W R_0 (\rho_0 - F_0) R_0 W^\dagger K^\dagger &= K W R_0 \rho_0 R_0^\dagger W^\dagger K^\dagger - K W R_0 \sqrt{\rho_0} U \sqrt{\rho_0} R_0^\dagger W^\dagger K^\dagger T \\ &= K W P A^2 P W^\dagger K^\dagger - K W P A U A P W^\dagger K^\dagger T \\ &= e^{\frac{-\mu}{2}} \begin{pmatrix} \text{Cosh}(\frac{\mu}{2}) - \text{Cos}^2(\frac{\mu}{2}) & 0 & 0 & -i \text{Sin}^2(\mu) \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ i \text{Sin}^2(\mu) & 0 & 0 & \text{Sinh}(\frac{\mu}{2}) - \text{Sin}^2(\frac{\mu}{2}) \end{pmatrix}. \end{aligned} \quad (6.105)$$

We are very closed to find the spectrum of $\rho_0 - F_0$. We can denote by M the previous matrix. The eigenvalues of this matrix M are given by the roots of the polynomial $P(x) = x^2 - \text{Tr}(M)x + \text{Det}(M)$ which simply are

$$x_{\pm} = \frac{1}{2} \left(\text{Tr}(M) \pm \sqrt{\text{Tr}(M)^2 - 4 \text{Det}(M)} \right). \quad (6.106)$$

All this complicated construction was necessary to obtain the spectrum of the operator $\rho_0 - F_0$. We victoriously end up with

$$\text{Spect}(\rho_0 - F_0) = \frac{1}{2} \left(1 - e^{\frac{-\mu}{2}} \pm e^{-\mu} \sqrt{1 + e^{\mu} - 2e^{\frac{\mu}{2}} \text{Cos}(\mu)} \right). \quad (6.107)$$

This spectrum is not always positive (see Fig. 6.6).

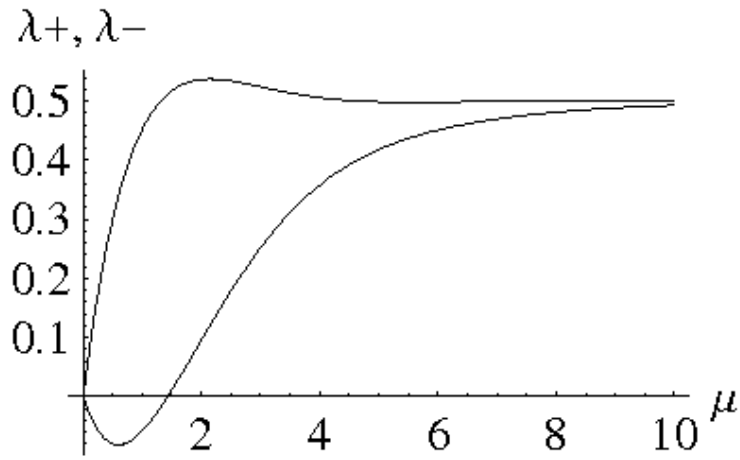
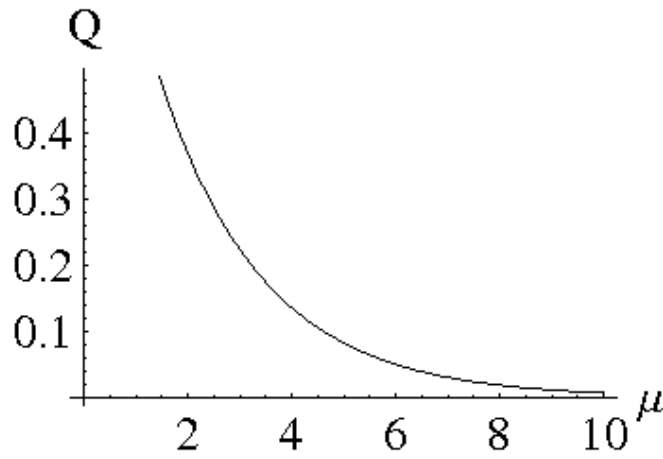
Only in the regime of relatively large μ , the quantity $\frac{1}{2}(1 - e^{\frac{-\mu}{2}} - e^{-\mu} \sqrt{1 + e^{-\mu} - 2e^{\frac{-\mu}{2}} \text{Cos}(\mu)})$ is greater than 0. More precisely,

$$\text{Spect}(\rho_0 - F_0) \geq 0 \Leftrightarrow \mu \geq \mu_0 \approx 1.4386 \quad (6.108)$$

where μ_0 is the solution of the equation $\frac{1}{2} \left(1 - e^{\frac{-\mu}{2}} - e^{-\mu} \sqrt{1 + e^{-\mu} - 2e^{\frac{-\mu}{2}} \text{Cos}(\mu)} \right) = 0$.

In the regime $\mu \geq \mu_0$ (see Fig. 6.7), the optimal failure probability reaches the overall lower bound and we therefore get

$$Q = F = \text{Tr}(F_0) = e^{\frac{-\mu}{2}}. \quad (6.109)$$

Figure 6.6: Spectrum of the operator $\rho_0 - F_0$ for USD of the *bit value* mixed statesFigure 6.7: Optimal failure probability for USD of the *bit value* mixed states for $\mu \geq \mu_0$

The corresponding optimal measurement is moreover given by

$$\begin{aligned} E_0 &= \Sigma^{-1} \sqrt{\rho_0} (\rho_0 - F_0) \sqrt{\rho_0} \Sigma^{-1} \\ E_1 &= U E_0 U \\ E_? &= \mathbb{1} - E_0 - U E_0 U. \end{aligned} \tag{6.110}$$

Note that for $\mu = \mu_0$, the POVM elements E_0 and E_1 have rank 1 since one eigenvalue of $\rho_0 - F_0$ vanishes.

We can remark here again that if we wanted to unambiguously discriminate

$$\rho_0 = \frac{1}{2}(|\alpha\rangle\langle\alpha| + |i\alpha\rangle\langle i\alpha|) \quad (6.111)$$

$$\text{and } \rho_1 = \frac{1}{2}(|-\alpha\rangle\langle-\alpha| + |-i\alpha\rangle\langle-i\alpha|). \quad (6.112)$$

then we would find for $\mu \geq 0.7193$

$$Q = e^{-\mu}. \quad (6.113)$$

In the regime $\mu \leq \mu_0$ where the operator $\rho_0 - F_0$ is not positive, we have to check the spectrum of the operator $P_1^\perp U P_1^\perp$. It is actually, as far as we know, not possible to calculate analytically its spectrum. Even if it is not really satisfying, we compute numerically the spectrum of $P_1^\perp U P_1^\perp$. It turns out that it always has two eigenvalues of opposite sign in the regime $\mu \leq \mu_0$. Consequently, we can write the operator $P_1^\perp U P_1^\perp$ in its eigenbasis $\{|0\rangle, |1\rangle\}$ as

$$P_1^\perp U P_1^\perp = a|0\rangle\langle 0| - b|1\rangle\langle 1|, \quad a, b \in \mathbb{R}^+. \quad (6.114)$$

And in virtue of Theorem 19, the optimal failure probability (see Fig. 6.8) for unambiguously discriminating the *bit value* mixed states is

$$Q^{\text{opt}} = 1 - \frac{1}{a+b}(b\langle 0|\rho_0|0\rangle + a\langle 1|\rho_0|1\rangle + 2\sqrt{ab}|\langle 0|\rho_0|1\rangle|). \quad (6.115)$$

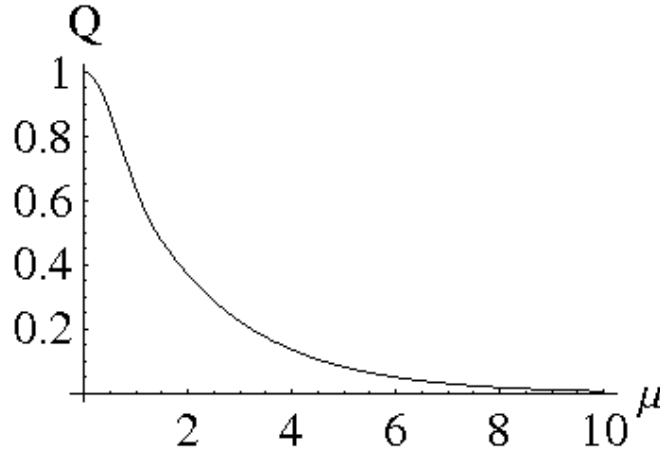


Figure 6.8: Optimal failure probability for USD of the *bit value* mixed states

So far, no neat expression in terms of μ is known for this optimal failure probability Q^{opt} for $\mu \leq \mu_0$ even if we do know its structure. This comes from the rather complicated form of the

states ρ_0 and ρ_1 . As a final word, let us add that the optimal USD measurement is of form

$$\begin{aligned} E_0 &= |x\rangle\langle x| \\ E_1 &= UE_0U \\ E_? &= \mathbb{1} - E_0 - UE_0U \end{aligned} \quad \text{with } |x\rangle = \begin{pmatrix} \frac{e^{-i\text{Arg}(\langle 1|\rho_0|0\rangle)}}{\sqrt{1+a/b}} \\ \frac{1}{\sqrt{1+b/a}} \\ 0 \\ 0 \end{pmatrix}, \quad (6.116)$$

even here also, we can note write them in term of the mean photon number μ . On the last graph 6.9, we can show and compare the two optimal failure probabilities derived in this chapter.

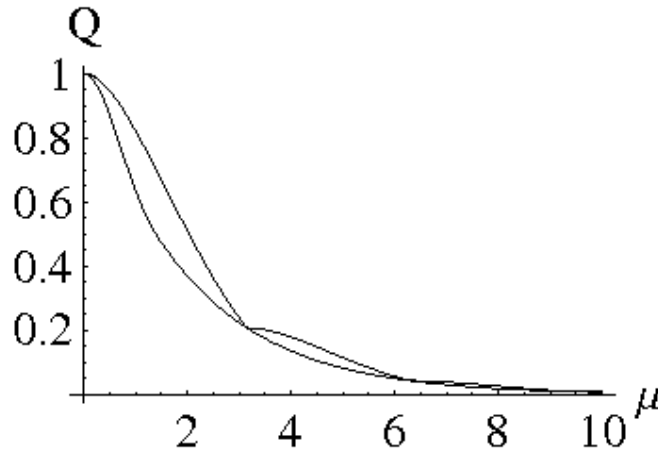


Figure 6.9: Comparison between the optimal failure probabilities for USD of the *basis* and the *bit value* mixed states

This conclude the last chapter of this thesis.

This last example might appear a bit unsatisfactory to the reader since no analytical expression for $P_1^\perp U P_1^\perp$ is known. However this is exactly the contrary. During my work on Unambiguous State Discrimination, I was guided by the four density matrices presented in this chapter. They were my inspiration as well as my life ring. They are actually at the core of the derivation of the two classes of exact solutions and the numerous theorems derived in this thesis would not have been found without them.

Chapter 7

Epilogue

The main results of this thesis are, first, the two classes of exact solutions, second the reduction theorems, and finally the solution to unambiguous comparison of n pure states having some simple symmetry and the application of our results on USD to a BB84-type protocol.

There are actually two directions for research in USD. The first path is of course the derivation of new solutions. The second is to find new applications of the already known solutions. In this thesis, we have tried to follow both paths. On one hand, we have derived new tools and new classes of exact solutions. On the other hand, we have given two examples of application for our tools.

With respect to the newly developed tools, we have presented the notion of parallel addition $\rho_0 \Sigma^{-1} \rho_1$ in the context of unambiguous state discrimination. We have also shown the relevance of the two operators $\sqrt{\sqrt{\rho_0} \rho_1 \sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1} \rho_0 \sqrt{\rho_1}}$. We have finally provided two new classes of exact solutions as well as the three reduction theorems as we now discuss.

The two classes of exact solutions derived in this thesis are the only two analytical solutions for unambiguous discrimination of two generic density matrices known so far. There now exist six analytical solutions for optimal unambiguous discrimination of quantum states. They correspond to the unambiguous discrimination of:

1. Any set of linearly independent symmetric pure states [19].
2. Any pair of nonoverlapping mixed states¹ such that the two operators $\rho_0 - \alpha \sqrt{\sqrt{\rho_0} \rho_1 \sqrt{\rho_0}}$ and $\rho_1 - \frac{1}{\alpha} \sqrt{\sqrt{\rho_1} \rho_0 \sqrt{\rho_1}}$ are positive semi-definite, and where α depends on the regime of the ratio $\sqrt{\frac{\eta_1}{\eta_0}}$ [chapter 4]. Note that the case of 'Any pair of two pure states' solved by Jaeger and

¹Any USD problem of two density matrices can be reduced to such a form according to Theorem 9.

Shimony [17] is included in this class of solutions.

3. Any pair of geometrically uniform mixed states of rank two in a four-dimensional Hilbert space [chapter 5]. We find that only three options for the expression of the failure probability exist. First, if the operator $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0$ is positive semi-definite, then the pair of density matrices falls in the first class of exact solutions. If this is not the case, either the operator $P_1^\perp U P_1^\perp$ has one positive and one negative eigenvalue or it has two eigenvalues of the same sign. In the former case, we can give the optimal failure probability in terms of the eigenvalues and eigenvectors of $P_1^\perp U P_1^\perp$. In the later case, no unambiguous discrimination is possible and the failure probability simply equals unity.

4. A pure state and a density matrix with arbitrary *a priori* probabilities [34].

5. Any pair of mixed states with one-dimensional kernel [26].

6. Any pair of subspaces [35].

Note that for the classes 2 and 3, we provide the optimal failure probability as well as the optimal measurement. Moreover, the solutions 4, 5 and 6 are reducible to some pure-state solutions. As we showed in this thesis, the reduction theorems and the solution for USD of two pure states are sufficient to derive those three solutions.

The three reduction theorems allow us to reduce USD problems to simpler cases for which the solution might be known. This is the case, as we showed in chapter 3, for the *unambiguous comparison of two pure states* [27, 28, 29], the *unambiguous comparison of n pure states having some simple symmetry*², *state filtering* [33, 34] and the *unambiguous discrimination of two subspaces* [35]. The reduction theorems also permit us to define a so-called standard USD problem. This problem is concerned with two density matrices of the same rank r in a $2r$ -dimensional Hilbert space. This is proposed as a starting point for further investigations in unambiguous state discrimination in order to avoid trivial cases or unnecessary complexity. The reductions come from simple geometrical considerations and can be summarized as follows. With the first reduction theorem, we split off any common subspace between the supports of the two density matrices ρ_0 and ρ_1 . Thanks to the second reduction theorem, we eliminate, if present, the part of the support of ρ_1 which is orthogonal to the support of ρ_0 and *vice versa*. With the third reduction theorem, if two density matrices are block diagonal, we decompose the global USD problem into decoupled unambiguous discrimination tasks on each block. These three reduction theorems are also used to derive general theorems on unambiguous state

² n linearly independent pure states with equal *a priori* probabilities and equal and real overlaps.

discrimination. For example, the first reduction theorem is required to derive the two classes of exact solutions since the assumption of two density matrices without overlapping supports is made.

With respect to the applications, we have used our new tools for the unambiguous comparison of n pure states with a simple symmetry³ and to answer two crucial questions⁴ related to the implementation of the Bennett-Brassard 1984 Quantum Key Distribution protocol. In fact we prove that the comparison of n linearly independent pure states with equal *a priori* probabilities and equal and real overlaps, a task related to the USD of two density matrices, can be reduced to n unambiguous discriminations of two pure states and can then be solved. The question to know whether any unambiguous comparison of pure states is always reducible to some pure state cases remains open⁵. With respect to the BB84-type protocol implemented with weak coherent pulses and a phase reference, we give the probability with which an eavesdropper can unambiguously distinguish the *basis* of the signal as well as the probability with which an eavesdropper can unambiguously determine which *bit value* is sent without being interested in the knowledge of the basis.

Finally, as we discussed in chapter 5, a unified expression for the failure probability for the second class of exact solutions might be a pre-condition to find new solutions in unambiguous discrimination of two density matrices. Moreover new consequences of Theorem 18 should be investigated.

³ n linearly independent pure states with equal *a priori* probabilities and equal and real overlaps.

⁴First 'With what probability can an eavesdropper unambiguously distinguish the *basis* of the signal?' and second 'With what probability can an eavesdropper unambiguously determine which *bit value* is sent without being interested in the knowledge of the basis?'.

⁵while the unambiguous comparison of mixed states is generally not reducible to some pure states case [28]

Chapter 8

Appendix

8.1 Appendix A

Theorem 20 *Theorem For any operator A ,*

$$A^\dagger A|x\rangle = 0 \Leftrightarrow A^\dagger |x\rangle = 0. \quad (8.1)$$

Proof We show this equivalence by proving separately the two implications.

\Leftarrow] This direction is trivial. If $A|x\rangle = 0$ then $A^\dagger A|x\rangle = 0$.

\Rightarrow] Here we make use of a fundamental theorem of linear algebra for any linear map A , the kernel of A^\dagger equals the orthogonal complement of the image of A that is to say $\text{Ker}(A^\dagger) = \text{Im}(A)^\perp$. Let us start with a vector $|x\rangle$ such that $A^\dagger A|x\rangle = 0$. $A|x\rangle$ is in the kernel of A^\dagger so that $A|x\rangle$ is in $\text{Im}(A)^\perp$. Moreover, by definition, $A|x\rangle$ is in $\text{Im}(A)$. It implies that $A|x\rangle = 0$. This completes the proof. ■

8.2 Appendix B

Proof of Lemma 2 For any operator A , we can introduce a polar decomposition $A = |A|V$ with $|A| = \sqrt{AA^\dagger} = V\sqrt{A^\dagger A}V^\dagger$. Note that V is unitary and not necessarily unique, while $\sqrt{AA^\dagger}$ and $\sqrt{A^\dagger A}$ are unique and positive semi-definite. Moreover, since $|A|$ might not have full rank, let us introduce the unitary transformation $V' = ZV$ where Z is a unitary matrix of the form

$$Z = \begin{pmatrix} \mathbb{1}_{\mathcal{S}_{|A|}} & 0 \\ 0 & T \end{pmatrix} \quad (8.2)$$

and T , a unitary matrix having support on $\mathcal{S}_{|A|}^\perp$. From this remark, it follows that if $A = |A|V$ is a valid polar decomposition then $A = |A|V'$ is as well a valid polar decomposition. Indeed, $A = |A|V' = |A|V$ and $|A| = V'\sqrt{A^\dagger A}V'^\dagger = V\sqrt{A^\dagger A}V^\dagger$.

We can now introduce a polar decomposition of A in the quantity $\text{Tr}(AW)$ and find

$$|\text{Tr}(AW)| = |\text{Tr}(|A|VW)| = |\text{Tr}(|A|^{1/2}|A|^{1/2}VW)|. \quad (8.3)$$

We denote $X = |A|^{1/2} = X^\dagger$ and $Y = |A|^{1/2}VW$ (W and V are both unitary matrices) and apply the Cauchy-Schwarz inequality (Theorem 2) to obtain

$$|\text{Tr}(AW)| = |\text{Tr}(X^\dagger Y)| \leq \sqrt{\text{Tr}(|A|)} \sqrt{\text{Tr}(W^\dagger V^\dagger |A| VW)} = \text{Tr}(|A|). \quad (8.4)$$

Equality holds if and only if $|A|^{1/2} = \beta |A|^{1/2}VW$, for some $\beta \in \mathbb{C}$. This is possible if and only if $\beta VW = R$, where R is of the same form than the unitary Z in Eqn. (8.2). We can multiply each side with its adjoint and then find $|\beta|^2 = 1$. This implies that $\beta = e^{-i\phi}$ for some angle ϕ so that we find the connection $W = V^\dagger R e^{i\phi}$. Since V comes from a polar decomposition of $|A|$ and R is of the form of T , W^\dagger is a valid unitary for a polar decomposition of $|A|$. This completes the proof. ■

8.3 Appendix C

Proof of Lemma 3 To complete the proof, we see two basic properties of the supports of two positive semi-definite matrices M and N

$$\mathcal{S}_{MN} \subset \mathcal{S}_M, \quad (8.5)$$

$$\mathcal{S}_M \subset \mathcal{S}_{M+N}. \quad (8.6)$$

The first ingredient is to see that $A : B$ is Hermitian. Indeed, we can write

$$A(A+B)^{-1}B = A(A+B)^{-1}(B+A-A) \quad (8.7)$$

$$= A(A+B)^{-1}(A+B) - A(A+B)^{-1}A. \quad (8.8)$$

Let us underline that $A(A+B)^{-1}(A+B) = A\Pi_{\mathcal{S}_{A+B}} = A$ since $\mathcal{S}_A \subset \mathcal{S}_{A+B}$. Similarly $(A+B)(A+B)^{-1}A = \Pi_{\mathcal{S}_{A+B}}A = A$. As a result,

$$A(A+B)^{-1}B = A - A(A+B)^{-1}A \quad (8.9)$$

$$= (A+B)(A+B)^{-1}A - A(A+B)^{-1}A \quad (8.10)$$

$$= A(A+B)^{-1}B. \quad (8.11)$$

Now we can prove that $\mathcal{S}_{A:B} \subset \mathcal{S}_A \cap \mathcal{S}_B$. Indeed $\mathcal{S}_{A(A+B)^{-1}B} \subset \mathcal{S}_A$ and $\mathcal{S}_{B(A+B)^{-1}A} \subset \mathcal{S}_B$. Since $A(A+B)^{-1}B = B(A+B)^{-1}A$, it follows that $\mathcal{S}_{A:B} \subset \mathcal{S}_A \cap \mathcal{S}_B$.

The last step is to prove that $\mathcal{S}_A \cap \mathcal{S}_B \subset \mathcal{S}_{A:B}$. To do so, let x be in $\mathcal{S}_A \cap \mathcal{S}_B$ and find a vector $y \in \mathcal{S}_A \cup \mathcal{S}_B$ such that $(A : B)y = x$. Actually, such a y is given by $(A^{-1} + B^{-1})x$. Indeed

$$(A : B)y = A(A+B)^{-1}B(A^{-1} + B^{-1})x \quad (8.12)$$

$$= B(A+B)^{-1}AA^{-1} + A(A+B)^{-1}BB^{-1}x \quad (8.13)$$

$$= B(A+B)^{-1}x + A(A+B)^{-1}x \quad (8.14)$$

since, $\forall x \in \mathcal{S}_A \cap \mathcal{S}_B$, $AA^{-1}x = x$ and $BB^{-1}x = x$. Finally we can write $(A : B)y = (B + A)(A + B)^{-1}x = x$ since $x \in \mathcal{S}_A \cap \mathcal{S}_B \subset \mathcal{S}_{A+B}$. These completes the proof. ■

Bibliography

- [1] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge, New Jersey, 3rd edition, 2000.
- [2] K. Kraus. *States, Effects, and Operations*. Number 190 in Lecture Notes in Physics. Springer, Berlin, 1983.
- [3] C. W. Helstrom. *Quantum detection and estimation theory*. Academic Press, New York, 1976.
- [4] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer, Dordrecht, 1993.
- [5] M. A. Naimark. Spectral functions of a symmetric operator. *Izv. Akad. Nauk SSSR, Ser. Mat.* , 4:277–318, 1940. Russian.
- [6] B. Sz-Nagy. *Extensions of linear transformations in Hilbert space which extend beyond this space*. Functional Analysis, Frederick Ungar, New York, supplement to f. riez and b. sz-nagy edition, 1960.
- [7] A. Chefles. Quantum state discrimination. *Contemporary Phys.*, 41(6):401, 2000.
- [8] S. Massar and S. Popescu. Optimal extraction of information from finite ensembles. *Phys. Rev. Lett.*, 74:1259, 1995.
- [9] D. Bruss and C. Macchiavello. Optimal state estimation for d -dimensional quantum systems. *Phys. Lett. A*, 253:249–251, 1999.
- [10] A. S. Holevo. Information theoretical aspects of quantum measurement. *Probl. Inf. Trans.*, 9:110–118, 1973.
- [11] R. Jozsa, D. Robb, and W. K. Wootters. Lower bound for accessible information in quantum mechanics. *Phys. Rev. A*, 49:273–279, 1994.
- [12] C. A. Fuchs. *Distinguishability and Accessible Information in Quantum Theory*. PhD thesis, University of Mexico, Mexico, 1995.

- [13] A. K. Ekert, B. Huttner, and G. M. Peres. Eavesdropping on quantum-cryptographical systems. *Phys. Rev. A*, 50(2):1047–1056, aug 1994.
- [14] D. Dieks. Overlap and distinguishability of quantum states. *Phys. Lett. A*, 126:303, 1988.
- [15] I. D. Ivanovic. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 123:257, 1987.
- [16] A. Peres. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 128:19, 1988.
- [17] G. Jaeger and A. Shimony. Optimal distinction between two non-orthogonal quantum states. *Phys. Lett. A*, 197:83–87, 1995.
- [18] A. Chefles. Unambiguous discrimination between linearly independent quantum states. *Phys. Lett. A*, 239(6):339–347, 1998.
- [19] A. Chefles and S. M. Barnett. Optimum unambiguous discrimination between linearly independent symmetric states. *Phys. Lett. A*, 250:223–229, 1998.
- [20] A. Peres and D. R. Terno. Optimal distinction between non-orthogonal quantum states. *J. Phys. A:Math. Gen.*, 31:7105, 1998.
- [21] X. M. Sun, S. Y. Zhang, Y. Feng, and M. S. Ying. Mathematical nature of and a family of lower bounds for the success probability of unambiguous discrimination. *Phys. Rev. A*, 65:0404306, 2002.
- [22] Y.C. Eldar. A semidefinite programming approach to optimal unambiguous discrimination of quantum states. *IEEE Trans.Inf. Theory*, 49:446, 2003.
- [23] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review*, 38:49, 1996.
- [24] L. Vandenberghe and S. Boyd. *Convex Optimization*. Cambridge University Press, 2004.
- [25] A. Ben-Tal and A. Nemirovski. *Lectures on Modern Convex Optimization*. MPS/SIAM Series on Optimization, Philadelphia, 2001.
- [26] T. Rudolph, R. W. Spekkens, and P. S. Turner. Unambiguous discrimination of mixed states. *Phys. Rev. A*, 68:010301(R), 2003.
- [27] S.M. Barnett, A. Chefles, and I. Jex. Comparison of two unknown pure quantum states. *Phys. Lett. A*, 307:189–195, 2003.
- [28] M. Kleinmann, H. Kampermann, and D. Bruss. Generalization of quantum-state comparison. *Phys. Rev. A*, 72:032308, 2005.

- [29] U. Herzog and J.A. Bergou. Optimum unambiguous discrimination of two mixed quantum states. *Phys. Rev. A*, 71:050301(R), 2005.
- [30] J. Jex, E. Andersson, and A. Chefles. Comparing the states of many quantum systems. *J. Mod. Opt.*, 51:505, 2004.
- [31] A. Chefles, E. Andersson, and J. Jex. Unambiguous comparison of the states of multiple quantum systems. *J. Phys. A*, 37:7315, 2004.
- [32] Y. Sun, J. A. Bergou, and M. Hillery. Optimum unambiguous discrimination between subsets of nonorthogonal quantum states. *Phys. Rev. A*, 66:032315, 2002.
- [33] J. A. Bergou, U. Herzog, and M. Hillery. Quantum filtering and discrimination between sets of boolean functions. *Phys. Rev. Lett.*, 90:257901, 2003.
- [34] J.A. Bergou, U. Herzog, and M. Hillery. Optimal unambiguous filtering of a quantum state: An instance in mixed state discrimination. *Phys. Rev. A*, 71:042314, 2005.
- [35] J. A. Bergou, E. Feldman, and M. Hillery. Optimal unambiguous discrimination of two subspaces as a case in mixed-state discrimination. *Phys. Rev. A*, 73:032107, 2006.
- [36] Y. C. Eldar, M. Stojnic, and B. Hassabi. Optimal quantum detectors for unambiguous detection of mixed states. *Phys. Rev. A*, 69:062318, 2004.
- [37] U. Herzog and J.A. Bergou. Distinguishing mixed quantum states: Minimum-error discrimination versus optimum unambiguous discrimination. *Phys. Rev. A*, 70:022302, 2004.
- [38] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, pages 175–179, New York, dec 1984. IEEE.
- [39] M. Dušek, M. Jahma, and N. Lütkenhaus. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Phys. Rev. A*, 62:022306, 2000.
- [40] R. Jozsa. Fidelity for mixed quantum states. *J. Mod. Opt.*, 41:2315–2323, 1994.
- [41] A. Uhlmann. The "transition probability" in the state space of a $*$ -algebra. *Reports on Mathematical Physics*, 9:273–279, 1976.
- [42] Y. Feng, R. Duan, and M. Ying. Unambiguous discrimination between mixed quantum states. *Phys. Rev. A*, 70:012308, 2004.
- [43] C Zhang, Y. Feng, and M. Ying. Unambiguous discrimination of mixed states. *quant-ph/0410073*, 2004.

- [44] G. Marsaglia and G.P.H. Styan. When does $\text{rank}(a+b)=\text{rank}(a)+\text{rank}(b)$? *Canad. Math. Bull.*, 15(3):451–452, 1972.
- [45] Ph. Raynal, N. Lütkenhaus, and S.J. van Enk. Reduction theorems for optimal unambiguous state discrimination of density matrices. *Phys. Rev. A*, 68:022308, 2003.
- [46] H. Barnum, C.M. Caves, C.A. Fuchs, R. Jozsa, and Schumacher. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett.*, 76:2818–2821, 1996.
- [47] P. Lancaster and M. Tismenetsky. *The Theory of Matrices, 2nd edition with applications*. Computer Science and Applied Mathematics. Academic Press, Inc., San Diego, 1985.
- [48] W.N. Jr. Anderson and R.J. Duffin. Series and parallel addition of matrices. *J. of Math. Analysis and Appl.*, 26:576–594, 1969.
- [49] J.A. Fill and D.E. Fishkind. The moore–penrose generalized inverse for sums of matrices. *SIAM. J. on Matrix Analysis and Appl.*, 21(2):629–638, 1998.
- [50] Y.C. Eldar and G.D. Forney. On quantum detection and the square-root measurement. *IEEE Trans. Inf. Theory*, 47(3):858–872, 2001.
- [51] Y.C. Eldar, A. Megretski, and G.C. Verghese. On quantum detection and the square-root measurement. *quant-ph/0211111*.
- [52] Y. C. Eldar. Mixed-quantum-state detection with inconclusive results. *Phys. Rev. A*, 67:042309, 2003.
- [53] Y.C. Eldar and H. Bolcskei. Geometrically uniform frames. *IEEE Trans. Inf. Theory*, 49:993, 2003.

Curriculum Vitae

Persönliche Daten

Geburtsdatum: 05.02.1978
Geburtsort: Lyon, Frankreich

Studium und Praktika

Abitur 1995

Diplom-Ingenieur an der Ecole Centrale de Marseille, Marseille, Frankreich 1998-2001
ex Ecole Nationale Supérieure de Physique de Marseille

Praktikum im Laboratoire de Physique Nucléaire et des Hautes Énergies, École Polytechnique, Paris, Frankreich Jul.-Sept. 2000

Betreuer des Praktikums: Dr. Arnd Specka

Thema des Praktikums: Elaboration of a calorimeter for HERA (DESY, Hamburg, Deutschland)

Praktikum im Institut Fresnel, Marseille, Frankreich Sept. 1999-Jul. 2000

Betreuer des Praktikums: Prof. Dr. Michel Lequime

Thema des Praktikums: Experimental Study of the laser ablation of a PVC surface

Praktikum im Laboratoire d'Astronomie Spatiale, Marseille, Frankreich Jul.-Sept. 2000

Betreuer des Praktikums: Dipl.-Ing. Philippe Lamy

Thema des Praktikums: Energy Cartography of the Sun

Diplomarbeit am Centre de Physique Théorique, Marseille, Frankreich 2000-2001

Diplomvater: Dr. C. Rovelli

Thema der Diplomarbeit: Introduction to 2d manifold-independent spinfoam theory

Promotionsstudium am Institut für Theoretische Physik I und am Institut für Optik, Max-Planck-Forschungsgruppe, Universität Erlangen-Nürnberg, Erlangen, Deutschland seit 2002